Some basic concepts of Number Theory and Modular Arithmetic

Greatest Common Divisor

The greatest common divisor (gcd) of numbers $a, b \in Z$ is the greatest integer that divides both a and b:

$$\gcd(a,\ b) = \max\{k \in Z |\ k|a \text{ and } k|b\}$$

Examples.

$\gcd(18,12) = 6$

$\gcd(13,10) = 1$

$\gcd(360,36) = 36$

If $a \neq 0$, then $\gcd(a, 0) = \gcd(0, a) = |a|$.

If $a \neq 0$ or $b \neq 0$, then

- $\gcd(a, b) = \gcd(b, a)$ and
- $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$

If $\gcd(a, b) = 1$, then numbers a and b are coprimes or *relatively prime*.

Example.

$\gcd(0,0)$ is not defined

$\gcd(20,9) = 1$ therefore 20 and 9 are coprimes

$\gcd(42,7) = \gcd(-42,7) = \gcd(42, -7) = \gcd(-42, -7) = 7$

$\gcd(130,25) = \gcd(25,130) = 5$

Prime numbers and compound numbers

Each number $a \in Z_+$ has trivial factors 1 and a. Other factors of a are called proper factors.

Note. For every a: $0|a \Leftrightarrow a = 0$. It means that 0 is only a factor of 0.

A natural number $p > 1$ is a prime number if it only has trivial factors 1 and p. Other natural numbers are compound numbers. Number 1 is neither a prime nor a compound number.

The set of primes is denoted by $P = \{2,3,5,7,11,13,17,19,23,29,31,37,41 \dots\}$ If $p \in P$ is a factor of a, it is called a prime factor of a.

Example. Number 24 has factors 1,2,3,4,6,8,12 ja 24, of which

- 1 and 24 are trivial
- 2 and 3 are prime

Example. Number 24 is a compound number.

Number 29 has factors 1 and 29, which are both trivial factors. Hence $29 \in P$.

Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic

Every natural number $a > 1$ has a unique and unambiguous presentation as a product of prime numbers:

$$a = p_1^{e_1} \dots p_n^{e_n} = \Pi_{i=1}^{n} p_i,$$

where $p_1 \leq p_2 \leq \cdots \leq p_n$ and $e_i \geq 1$.

This is called the prime factorization of a.

Example. The prime factorization of 720:

$$720 = 2 \cdot 360 = 2^2 \cdot 180 = 2^3 \cdot 90 = 2^4 \cdot 45 = 2^4 \cdot 3 \cdot 15 = 2^4 \cdot 3^2 \cdot 5$$

Example. (Finding the gcd using the prime factorization)

To find $\gcd(60,36)$, we first find the prime factorizations of both 60 and 36:

$60 = 2 \cdot 30 = 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$ and

$36 = 2 \cdot 18 = 2 \cdot 2 \cdot 9 = 2^2 \cdot 3^2$.

Now, $\gcd(a, b)$ is the product of all common prime factors of a and b. So here we get

$$\gcd(60,36) = 2^2 \cdot 3 = 12$$

Example. Find $\gcd(935,228)$.

Prime factorizations: $935 = 5 \cdot 11 \cdot 17$ and $228 = 2^2 \cdot 3 \cdot 19$.

The numbers have no common factors, thus $\gcd(935,228) = 1$ and 935 and 228 are coprimes.

Modulo operation

Definition. Let $a, r \in Z$ and $m \in Z_+$. If $m \mid (a - r)$, then a and r are congruent modulo m, denote

$$a \equiv r \ (mod\ m)$$

Example. Some congruences modulo 12.

$13 \equiv 1 \ (mod\ 12)$ as $12 \mid (13 - 1)$

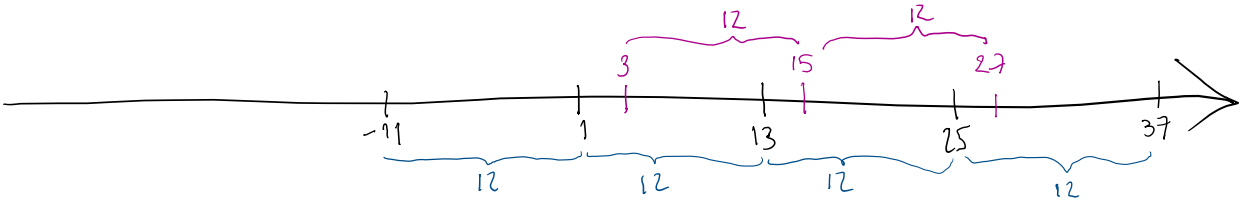
$13 \equiv 37 \ (mod\ 12)$ as $12 \mid (37 - 13)$

$13 \equiv -11 \ (mod\ 12)$ as $12 \mid (13 + 11)$

$13 \not\equiv 3 \ (mod\ 12)$ as $12 \nmid (13 - 3)$

$27 \equiv 3 \ (mod\ 12)$ as $12 \mid (27 - 3)$

Thus, numbers 1, 13, 37 and -11 are all congruent modulo 12. So are numbers 3, 15 and 27.



Division identity. Given any $a \in Z, m \in Z_+$, we can write a in form

$$a = q \cdot m + r$$

for some $q \in Z, r \in \{0,1, \dots, m-1\}$.

In terms of division: a is *dividend*, m is *divisor* (or *modulus*), q is *quotient* and r is *remainder*.

Note. Integers a and b are congruent modulo m, if they have the same remainder when divided by m.

Example.

$$13 = 1 \cdot 12 + 1$$

$$37 = 3 \cdot 12 + 1$$

$$-11 = -1 \cdot 12 + 1$$

$$3 = 0 \cdot 12 + 3$$

$$27 = 2 \cdot 12 + 3$$

Equivalence classes

Definition. Let $a \in Z$ and $m \in Z_+$. The equivalence class modulo m for number a is the set

$$\bar{a} = \{x \in Z \mid x \equiv a \pmod m\}$$

Note. There are m equivalence classes for modulus m, namely $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}$
All these together form a partition of Z, "integers modulo m":

$$Z_m = \{\bar{a} \mid a \in Z\}$$

Example. Equivalence classes modulo 12 are

$$\bar{0} = \{\dots, -24, -12, 0, 12, 24, \dots\}$$

$$\bar{1} = \{\dots, -23, -11, 1, 13, 25, \dots\}$$

$$\bar{2} = \{\dots, -22, -10, 2, 14, 26, \dots\}$$

$$\vdots$$

$$\overline{11} = \{\dots, -13, -1, 11, 23, 35, \dots\}$$

$\mathbb{Z}_{12}$

Computations in Z_m

In addition and in multiplication modulo m, any element of an equivalence class can be replaced by any other element of the same class. This means that we can choose an element which makes our computation as easy as possible.

Example.

In Z_6: $-18 + 601 = 583 \equiv 1\ (mod\ 6)$ **or** $-18 + 601 \equiv 0 + 1 = 1\ (mod\ 6)$

In Z_9: $8^{50} \equiv (-1)^{50} = 1\ (mod\ 9)$

$100^{99} = (10 \cdot 10)^{99} = 10^{99} \cdot 10^{99} \equiv 1^{99} \cdot 1^{99} = 1\ (mod\ 9)$

In Z_{12}: $5^9 = 1953125 \equiv 5\ (mod\ 12)$ **or**

$5^9 = 5^{2\cdot 4+1} = (5^2)^4 \cdot 5 = 25^4 \cdot 5 \equiv 1^4 \cdot 5 = 5\ (mod\ 12)$

Integer rings

Definition. The **integer ring** Z_m consists of

1) set $Z_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$

2) operations "+" and "·" for all $\bar{a}, \bar{b} \in Z_m$ such that

$\bar{a} + \bar{b} \equiv \bar{c}\ (mod\ m)$

$\bar{a} \cdot \bar{b} \equiv \bar{d}\ (mod\ m)$ where $\bar{c}, \bar{d} \in Z_m$.

Example.

In Z_9,

$\bar{2} + \bar{5} = \bar{7}$ $\bar{2} + \bar{8} = \bar{1}$ $\bar{2} \cdot \bar{8} = \bar{7}$

In Z_{12},

$\bar{2} + \overline{11} = \bar{1}$ $\bar{2} \cdot \overline{11} = \overline{10}$ $\bar{5} \cdot \bar{5} = \bar{1}$

Properties of rings. All integer rings have the following properties:

1) A ring is *closed* under operations "+" and "·".

2) Operations "+" and "·" are *associative*:
$(a + b) + c = a + (b + c)$
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3) There is a *neutral element* 0 wrt addition, for which
$a + 0 \equiv a \ (mod\ m)$ for all $a \in Z_m$.

4) There is a *neutral element* 1 wrt multiplication, for which
$a \cdot 1 \equiv a \ (mod\ m)$ for all $a \in Z_m$.

5) Every element $a \in Z_m$ has an *additive inverse* $-a$ such that
$a + (-a) \equiv 0 \ (mod\ m)$.

Example. In Z_{23}:

The neutral element wrt to addition is $\bar{0}$, as for any $\bar{a} \in Z_{23}$

$$\bar{0} + \bar{a} = \bar{a}$$

The neutral element wrt to multiplication is $\bar{1}$, as for any $\bar{a} \in Z_{23}$,

$$\bar{1} \cdot \bar{a} = \bar{a}$$

The additive inverse of 5 is 18, as $5 + 18 = 23 \equiv 0 \ (mod\ 23)$.
Hence, we denote $-5 = 18$ in Z_{23}.

The additive inverse of 6 is 17, as $6 + 17 = 23 \equiv 0 \ (mod\ 23)$.
Hence, we denote $-6 = 17$ in Z_{23}.

Multiplicative inverse

Definition. The multiplicative inverse of $a \in Z_m$ is denoted a^{-1} and defined as

$$a \cdot a^{-1} \equiv 1 \ (mod\ m)$$

If a^{-1} exists, then a is *invertible*.

Definition. If a has a multiplicative inverse in Z_m, then division $\frac{b}{a}$ is defined as

$$\frac{b}{a} = b \cdot a^{-1}$$

Note. For any given $a \in Z_m$, the multiplicative inverse exists if and only if

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

Example. In Z_{18}:

Element 5 is invertible, as $\gcd(5,18) = 1$.

The inverse $5^{-1} = 11$, as $5 \cdot 11 = 55 = 3 \cdot 18 + 1 \equiv 1 \ (mod\ 18)$.

Element 6 is not invertible, as $\gcd(18,6) = 6\ (\neq 1)$.

Element 7 is invertible, as $\gcd(7,18) = 1$.

The inverse $7^{-1} = 13$, as $7 \cdot 13 \equiv 7 \cdot (-5) = -35 \equiv 1 \ (mod\ 18)$.

Element 8 has no inverse, as $\gcd(18,8) = 2\ (\neq 1)$.

Galois fields and Galois Extension fields

Galois fields

Definition. Let $p \in P$. Then the integer ring Z_p is a finite field or a Galois field, also denoted $GF(p)$.

Note. All nonzero elements of $GF(p)$ have multiplicative inverses.

Example. Consider the smallest finite field $GF(2)$. Then

addition

multiplication

We note that

- addition in $GF(2)$ is equivalent to XOR operation
- multiplication in $GF(2)$ is equivalent to AND operation

Example. Consider Galois field $GF(5)$. Find the additive and multiplicative inverses in $GF(5)$.

addition:

multiplication:

Galois extension fields

Definition. A finite field $GF(p^m)$ where $p \in P, m \in N, m > 1$ is called a Galois extension field. The elements of $GF(p^m)$ are presented as *polynomials* of degree $m-1$ with coefficients in $GF(p)$.

Example. In $GF(2^8)$, the elements are polynomials of degree $8-1=7$ with coefficients in $GF(2)$.

$A \in GF(2^8)$: $\quad A(x) = a_7x^7 + a_6x^6 + \cdots + a_1x + a_0,$

where $a_i \in \{0,1\}$

Notation and storage for each element of $GF(2^8)$ takes one byte, f.ex.

$x^7 + x^5 + x^2 + x \quad \leftrightarrow \quad 10100110$

$x^6 + x^4 + 1 \quad \leftrightarrow \quad 01010001$

Addition in $GF(2^m)$

Definition. Let $A, B \in GF(2^m)$. Then

$$C(x) = A(x) + B(x) = \sum_{i=0}^{m-1} c_i x^i,$$

where $c_i \equiv a_i + b_i \ (mod\ 2)$.

Example. Find the sum of $A(x) = x^7 + x^6 + x^4 + 1$ and $B(x) = x^4 + x^2 + 1$ in $GF(2^8)$:

Note. In $GF(2^m)$, addition is equivalent to bitwise XOR.

Note. In $GF(2^m)$, subtraction is equivalent to addition.

Irreducible polynomials

Irreducible polynomials are polynomials which cannot be factored into products of other nontrivial polynomials.

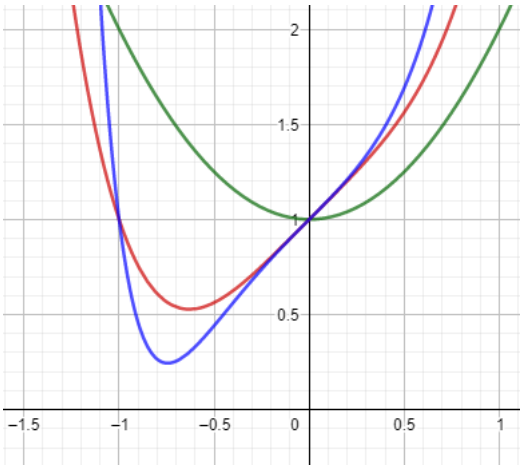
Example. Polynomial $x^2 + 1$ is irreducible.

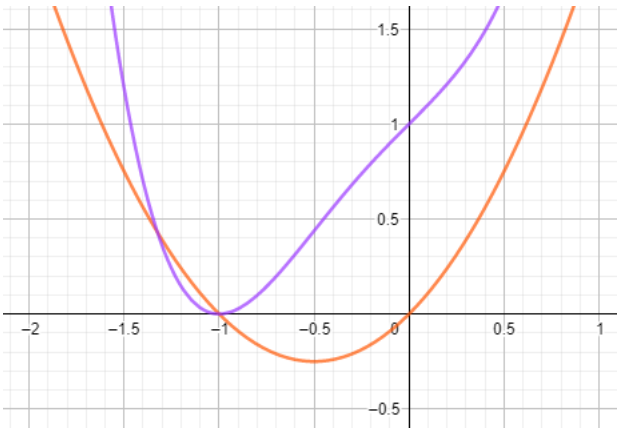
Polynomial $x^4 + x + 1$ is irreducible.

Polynomial $x^2 + x = x(x + 1)$ is not irreducible. It is *reducible*.

Polynomial $x^4 + x^3 + x + 1 = (x^3 + 1)(x + 1)$ is reducible.

Polynomial $x^8 + x^4 + x^3 + x + 1$ is irreducible.





Multiplication in $GF(2^m)$

Let us recall standard polynomial multiplication:

$C(x) = A(x) \cdot B(x)$, where $\deg C = \deg A + \deg B$

Example. Let $A(x) = x^3 + x^2 + 1$ and $B(x) = x^2 + x$. Then the product

$$\begin{aligned} C(x) &= A(x) \cdot B(x) \\ &= (x^3 + x^2 + 1)(x^2 + x) \\ &= x^5 + x^4 + x^4 + x^3 + x^2 + x \\ &= x^5 + 2x^4 + x^3 + x^2 + x \end{aligned}$$

For multiplication in $GF(2^m)$, we divide the product C by an irreducible polynomial P of degree m and consider only the remainder, for which the maximum degree is $m-1$. This is to make sure that the product C also is an element of $GF(2^m)$.

Definition. Let $A, B \in GF(2^m)$ and let $P(x) = \sum_{i=0}^{m} p_i x^i$, where $p_i \in \{0,1\}$ and $\deg P = m$, be an irreducible polynomial. Then

$$C(x) = A(x) \cdot B(x) \pmod{P}$$

Example. Multiply $A(x) = x^3 + x^2 + 1$ and $B(x) = x^2 + x$ in $GF(2^4)$ using the irreducible polynomial $P(x) = x^4 + x + 1$.

$$\begin{aligned} C(x) &= (x^3 + x^2 + 1)(x^2 + x) \\ &= x^5 + 2x^4 + x^3 + x^2 + x \\ &= x^5 + x^3 + x^2 + x \\ &= x(x^4 + x + 1) + x^3 \\ \\ &\equiv x^3 \pmod{P} \end{aligned}$$

Hence, $C(x) = x^3 \pmod{P}$.

Alternatively, you can find the product $A(x) \cdot B(x)$ using a table of coefficients, and then use polynomial division to find the remainder.

Note. For AES, the irreducible polynomial used in multiplications in $GF(2^8)$ is always

$$P(x) = x^8 + x^4 + x^3 + x + 1$$

Inversion in $GF(2^m)$

Definition. For given $GF(2^m)$ and the corresponding irreducible polynomial $P(x) \in GF(2^m)$, the inverse $A^{-1}$of a nonzero polynomial A is defined as

$$A^{-1} \cdot A = 1 \ (mod\ P)$$

Example. The inverse of $A(x) = x^3 + 1$ in $GF(2^4)$ with $P(x) = x^4 + x + 1$ is $A^{-1}(x) = x$.
Verification:

$$\begin{aligned} A \cdot A^{-1} &= (x^3 + 1)x \\ &= x^4 + x \\ &= x^4 + x + 1 + 1 \\ \\ &\equiv 1 \quad (mod\ P) \end{aligned}$$

Hence, $A^{-1}(x) = x$.

Example. The inverse of $B(x) = x^3 + x^2 + 1$ in $GF(2^4)$ with $P(x) = x^4 + x + 1$ is $B^{-1}(x) = x^2$.
Verification:

$$\begin{aligned} B \cdot B^{-1} &= (x^3 + x^2 + 1)x^2 \\ &= x^5 + x^4 + x^2 \end{aligned}$$

Dividing $x^5 + x^4 + x^2$ by P yields $x + 1$, remainder 1. Hence, $B \cdot x^2 = 1 \ (mod\ P)$ and therefore $B^{-1}(x) = x^2$.

Note. The inverse elements in $GF(2^m)$ can be found using the Euclidean algorithm for polynomials. For small fields (say, $m \leq 16$) it is customary to use lookup tables instead.

Below is the multiplicative inverse table in $GF(2^m)$ that is used within the AES S-box. For a byte xy, we interpret each set of four bits x and y as hexadecimal numbers which determine the row and column. We then find A^{-1} from the table as two hexadecimals and change it back to binary.

Multiplicative inverse table in $GF(2^8)$ for bytes xy used within the AES S-Box

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

Example. Finding the inverse for AES byte $A_0 = 10001101$ from the lookup table yields $A_0^{-1} = 00000010$.

To verify the result, we express the bytes as polynomials:
$A_0 = 10001101 \to x^7 + x^3 + x^2 + 1$, $A_0^{-1} = 00000010 \to x$.

Multiplying $mod\ P$:

$$\begin{aligned} A_0 \cdot A_0^{-1} &= (x^7 + x^3 + x^2 + 1)x \\ &= x^8 + x^4 + x^3 + x \\ &= (x^8 + x^4 + x^3 + x + 1) + 1 \\ &= P(x) + 1 \\ &\equiv 1 \quad (mod\ P) \end{aligned}$$

Example. Find the inverse of $A = 29_{16}$ from the lookup table.
Here, $x = 2$ and $y = 9$, Hence, $A^{-1} = 0A_{16}$.

To verify, we express the bytes as polynomials:
$A = 00101001 \to x^5 + x^3 + 1$ and $A^{-1} = 00001010 \to x^3 + x$.

Then

$$\begin{aligned} A \cdot A^{-1} &= (x^5 + x^3 + 1)(x^3 + x) \\ &= x^8 + x^6 + x^6 + x^4 + x^3 + x \\ &= x^8 + x^4 + x^3 + x \\ &= x^8 + x^4 + x^3 + x + 1 + 1 \\ &= P(x) + 1 \\ &\equiv 1 \qquad (mod\ P) \end{aligned}$$

Essential Number Theory for Public-Key Algorithms

Euclidean Algorithm (EA)

In general, it is not practical or feasible to use factorizations of numbers to find their gcd. Instead, we use the Euclidean algorithm:

Euclidean Algorithm
Input: positive integers r_0 and r_1 with $r_0 > r_1$
Output: $\gcd(r_0, r_1)$
Initialization: $i = 1$
Algorithm:

1 DO
1.1 $i = i + 1$
1.2 $r_i = r_{i-2} \bmod r_{i-1}$ find remainder of r_{i-2} (mod r_{i-1})
WHILE $r_i \neq 0$
2 RETURN
$\gcd(r_0, r_1) = r_{i-1}$

Note. EA is very efficient and always terminates. The number of iterations is close to the number of digits of the input operands.

Example. a) Find $\gcd(\overset{r_0}{3910}, \overset{r_1}{720})$ using EA. b) Find $\gcd(\overset{r_0}{12345}, \overset{r_1}{284})$ using EA.

a) $\overset{r_0}{3910} = 5 \cdot \overset{r_1}{720} + \overset{r_2}{310}$
$\overset{r_1}{720} = 2 \cdot \overset{r_2}{310} + \overset{r_3}{100}$
$\overset{r_2}{310} = 3 \cdot \overset{r_3}{100} + \overset{r_4}{10}$
$\overset{r_3}{100} = 10 \cdot \overset{r_4}{10} + \overset{r_5}{0}$
$\Rightarrow \gcd(\overset{r_0}{3910}, \overset{r_1}{720}) = \overset{r_4}{10}$

b) $\overset{r_0}{12345} = 43 \cdot \overset{r_1}{284} + \overset{r_2}{133}$
$\overset{r_1}{284} = 2 \cdot \overset{r_2}{133} + \overset{r_3}{18}$
$\overset{r_3}{133} = 7 \cdot \overset{r_4}{18} + \overset{r_5}{7}$
$\overset{r_4}{18} = 2 \cdot \overset{r_5}{7} + \overset{r_6}{4}$
$7 = 1 \cdot 4 + 3$
$4 = 1 \cdot 3 + 1$
$3 = 3 \cdot 1 + 0$
$\Rightarrow \gcd(12345, 284) = 1$ (coprimes)

Diophantine equation (DE)

Definition. Diophantine equation is an equation of the form

$$ax + by = c,$$

where $a, b, c, x, y \in Z$.

- A solution of $ax + by = c$ is an integer pair (x, y).
- Diophantine equation $ax + by = c$ has a solution, iff $\gcd(a, b) \mid c$

$180x + 52y = 8$
$\gcd(180, 52) = 4$, $4 \mid 8 \Rightarrow$ has a solution
$12345x + 284y = 1$
$\gcd(12345, 284) = 1$, $1 \mid 1 \Rightarrow$ has a solution
$10x - 20y = 9$
$\gcd(-20, 10) = 10$, $10 \nmid 9$
$\Rightarrow$ no solution

Extended Euclidean Algorithm (EEA)

Task. For given r_0, r_1, find $\gcd(r_0, r_1)$. Then solve the Diophantine equation

$$\gcd(r_0, r_1) = s \cdot r_0 + t \cdot r_1$$

for $s, t \in Z$.

- Main application of EEA in cryptography is to find inverses in Z_n or Galois fields.

Extended Euclidean Algorithm (EEA)
Input: positive integers r_0 and r_1 with $r_0 > r_1$
Output: $\gcd(r_0, r_1)$, as well as s and t such that $\gcd(r_0, r_1) = s \cdot r_0 + t \cdot r_1$.
Initialization:
$s_0 = 1 \quad t_0 = 0$
$s_1 = 0 \quad t_1 = 1$
$i = 1$
Algorithm:

1 DO
1.1 $i = i + 1$
1.2 $r_i = r_{i-2} \bmod r_{i-1}$
1.3 $q_{i-1} = (r_{i-2} - r_i)/r_{i-1}$
1.4 $s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$
1.5 $t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$
WHILE $r_i \neq 0$
2 RETURN
$\gcd(r_0, r_1) = r_{i-1}$
$s = s_{i-1}$
$t = t_{i-1}$

$r_0 \quad r_1$

Example. Solve equation $\gcd(180,52) = 180s + 52t$.

i	$r_{i-2} = q_{i-1} \cdot r_{i-1} + r_i$	$r_i = [s_i] \cdot r_0 + [t_i] \cdot r_1$
2	$180 = 3 \cdot 52 + 24$	$24 = [1] \cdot 180 + [-3] \cdot 52$
3	$52 = 2 \cdot 24 + 4$	$4 = 52 - 2 \cdot 24$ $= 52 - 2(1 \cdot 180 + (-3) \cdot 52)$ $= [-2] \cdot 180 + [7] \cdot 52$
4	$24 = 6 \cdot 4 + 0$	

Thus, $\gcd(180,52) = 4$ and $s = -2, t = 7$ is a solution to equation

$4 = 180s + 52t$

$90^{-1} \cdot x = 1 \pmod{8633}$

Example. Find 90^{-1} in Z_{8633}. $r_0 = n = 8633$ and $r_1 = 90$

i	$r_{i-2} = q_i \cdot r_{i-1} + r_i$	$r_i = [s] \cdot r_0 + [t] \cdot r_1$
2	$8633 = 95 \cdot 90 + 83$	$83 = [1] \cdot 8633 - [95] \cdot 90$ $1 \cdot r_0 - 95 \cdot r_1$
3	$90 = 1 \cdot 83 + 7$	$7 = 1 \cdot 90 - 1 \cdot 83$ $= 1 \cdot 90 - 1 \cdot (1 \cdot 8633 - 95 \cdot 90)$ $= [-1] \cdot 8633 + [96] \cdot 90$ $-1 \cdot r_0 + 96 \cdot r_1$
4	$83 = 11 \cdot 7 + 6$	$6 = 1 \cdot 83 - 11 \cdot 7$ $= 1 \cdot (1 \cdot r_0 - 95 \cdot r_1) - 11 \cdot (-1 \cdot r_0 + 96 \cdot r_1)$ $= 12 \cdot r_0 - 1151 \cdot r_1$
5	$7 = 1 \cdot 6 + 1$	$1 = 1 \cdot 7 - 1 \cdot 6$ $= 1 \cdot (-1 \cdot r_0 + 96 \cdot r_1) - 1 \cdot (12 \cdot r_0 - 1151 \cdot r_1)$ $= -13 \cdot r_0 + 1247 \cdot r_1$
6	$6 = 6 \cdot 1 + 0$	

Thus, $\underbrace{-13 \cdot 8633}_{\equiv 0 \pmod{8633}} + 1247 \cdot 90 = 1 \quad \| \pmod{8633}$

$1247 \cdot 90 = 1 \pmod{8633}$

$\Rightarrow 90^{-1} = 1247$ in $\mathbb{Z}_{8633}$

Euler's Phi Function

for all $n \in \mathbb{Z}_+$, $\varphi(n) \in \{1, \dots, n-1\}$

Definition. For $n \in Z_+$, Euler's Phi function or totient function $\varphi(n)$ denotes the number of coprimes for n in the set $\{1,\ 2,\ 3, \dots, n-1\}$.

Example. $\varphi(6) = 2$, since in $\{1, 2, 3, 4, 5\}$, numbers 1 and 5 are coprimes of 6 and 2,3 and 4 are not.

gcd(6,2) = 2, gcd(6,4) = 2, gcd(6,3) = 3

$\varphi(7) = 6$, since all numbers in $\{1, 2, 3, 4, 5, 6\}$ are coprimes of 7.

$\varphi(8) = 4$, since in $\{1, 2, 3, 4, 5, 6, 7\}$ numbers 1,3,5,7 are coprimes of 8, and 2,4,6 are not.

n = 1234

φ(n) ?

Notes.

- $\varphi(n)$ indicates the number of elements in Z_n which have multiplicative inverses.
- For $p \in P$, every nonzero element of Z_p has an inverse.
- For $p,\ q \in P$, we have the following formulae:
  - $\varphi(p) = p - 1$
  - $\varphi(p^k) = p^{k-1}(p-1)$
  - $\varphi(pq) = (p-1)(q-1)$

7, 67 ∈ P, so

φ(7) = 6

φ(67) = 66

φ(8) = φ(2³) = 2^{3-1} · (2-1) = 2² = 4

φ(125) = φ(5³) = 5^{3-1} · (5-1) = 100

φ(335) = φ(5 · 67) = (5-1) · (67-1) = 264

- For any $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$, where $p_1, \dots p_k \in P$:

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_1 - 1} \cdot (p_i - 1)$$

$\sum_{i=1}^{k} X_i = X_1 + X_2 + \dots + X_k$

$\prod_{i=1}^{k} X_i = X_1 \cdot X_2 \cdot \dots \cdot X_k$

Example. Find $\varphi(n)$ for $n = 6, 7, 8, 864$ using the given formulae.

$$\varphi(864) = \varphi(2^5 \cdot 3^3) = 2^{5-1} \cdot (2-1) \cdot 3^{3-1} \cdot (3-1) = 2^4 \cdot 1 \cdot 3^2 \cdot 2 = 288$$

Fermat's Little Theorem (FLT)

Fermat's Little Theorem is a number-theoretical result that is useful in many aspects of public-key cryptography, for example *primality testing*.

Theorem. Let $a \in Z$ and $p \in P$. Then

$$a^{p-1} \equiv 1 \ (mod\ p)$$

$22^6 \equiv 1 \pmod 7$, because $7 \in \mathbb{P}$ (7−1)

$13^4 \equiv 1 \pmod 5$, $5 \in \mathbb{P}$

$13^7 \not\equiv 1 \pmod 8$, $8 \notin \mathbb{P}$

Example. Number 2^{1000} is divided by 17. What is the remainder?

As $17 \in P$, FLT applies and hence we know that $2^{16} \equiv 1 \ (mod\ 17)$. (FLT)

We form the division identity for $\frac{1000}{16}$:

$$1000 = 62 \cdot 16 + 8$$

Using this to simplify 2^{1000} (mod 17):

$$\begin{aligned} 2^{1000} &= 2^{62 \cdot 16 + 8} \\ &= (2^{16})^{62} \cdot 2^8 \\ &\equiv 2^8 \\ &= 256 \\ &= 15 \cdot 17 + 1 \\ &\equiv 1 \ (mod\ 17) \end{aligned}$$

$(2^{16})^{62} \cdot 2^8 = 1^{62} \cdot 2^8$, $2^{16} \equiv 1 \pmod{17}$, $1^{62} = 1$

$a^{x \cdot y} = (a^x)^y$, $a^{x+y} = a^x \cdot a^y$

Rewriting FLT again as

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

$$a \cdot a^{p-2} \equiv 1 \ (mod\ p)$$

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

a^{-1} multipl. inverse of a mod p (or in $\mathbb{Z}_p$)

we see that actually

$$a^{p-2} \equiv a^{-1} \ (mod\ p)$$

Hence we can use FLT to find the inverse of a for a prime modulus.

Example. Let $p = 11$ and $a = 2$. As $p \in P$ and $a \in Z$, we can find the inverse of a by applying FLT:

$$\begin{aligned} a^{-1} &\equiv a^{p-2} \\ &= 2^{11-2} \\ &= 512 \\ &= 46 \cdot 11 + 6 \\ &\equiv 6 \ (mod\ 11) \end{aligned}$$

Verification: $2 \cdot 6 = 12 \equiv 1 \ (mod\ 11)$

Ex. $p = 23$, $a = 90$

Find inverse of 90 in $\mathbb{Z}_{23}$

By FLT:

$90^{-1} = 90^{23-2}$

$= 90^{21}$

$\equiv 11 \pmod{23}$

To check,

$90 \cdot 11 = 990$

$\equiv 1 \pmod{23}$

Euler's Theorem

Another theorem which is quite useful in public-key cryptography is called Euler's Theorem, also known as Euler's totient theorem. Note that Euler's Theorem is a *generalization* of Fermat's Little Theorem, meaning that it extends FLT to cover more cases.

Theorem. Let $a, m \in Z$ and $\gcd(a, m) = 1$. Then

$$a^{\varphi(m)} \equiv 1 \ (mod\ m)$$

Example. Because $\gcd(864,5) = 1$ and $\varphi(864) = 288$, we know that

$$5^{288} \equiv 1 \ (mod\ 864)$$

Example. Let us find $3^{90} \ (mod\ 23)$.

As $23 \in P$, we know that $\varphi(23) = 22$. Since $\gcd(23,3) = 1$, Euler's Theorem applies and thus we know that $3^{22} \equiv 1 \ (mod\ 23)$.
Using this to simplify the original expression:

$$\begin{aligned} 3^{90} &= 3^{22 \cdot 4 + 2} \\ &= (3^{22})^4 \cdot 3^2 \\ &\equiv 1^4 \cdot 9 \\ &= 9 \ (mod\ 23) \end{aligned}$$

Groups

Definition. *A* group *is a set of elements G together with an operation $\circ$ which combines two elements of G. A group has the following properties.*

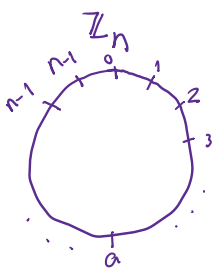
1. *The group operation $\circ$ is* closed. *That is, for all $a, b, \in G$, it holds that $a \circ b = c \in G$.*
2. *The group operation is* associative. *That is, $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$.*
3. *There is an element $1 \in G$, called the* neutral element *(or* identity element*), such that $a \circ 1 = 1 \circ a = a$ for all $a \in G$.*
4. *For each $a \in G$ there exists an element $a^{-1} \in G$, called the* inverse *of a, such that $a \circ a^{-1} = a^{-1} \circ a = 1$.*
5. *A group G is* abelian (or commutative) *if, furthermore, $a \circ b = b \circ a$ for all $a, b \in G$.*

Multiplicative groups Z_n^*

Definition. The multiplicative group Z_n^* of integer ring Z_n is

$$Z_n^* = \{a \in Z_n \mid \gcd(n, a) = 1\}$$

with operation $\cdot\ (mod\ n)$.



$a \in \{0,1,\dots,n-1\}$ such that n and a are coprimes ($\gcd(n,a) = 1$)

Example. $Z_6 = \{0,1,2,3,4,5\}$ (not coprimes with 6) $\qquad Z_6^* = \{1,5\}$

$Z_7 = \{0,1,2,3,4,5,6\} \qquad Z_7^* = \{1,2,3,4,5,6\}$

Note that $\gcd(n, a) = 1 \iff a$ has a multiplicative inverse in Z_n.

For example,

$Z_6 \rightarrow Z_6^*$

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$Z_7 \rightarrow Z_7^*$

*	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

Similarly, we have the following integer rings and their respective multiplicative groups:

$Z_8 = \{0,1,2,3,4,5,6,7\} \qquad Z_8^* = \{1,3,5,7\}$

$Z_9 = \{0,1,2,3,4,5,6,7,8\} \qquad Z_9^* = \{1,2,4,5,7,8\}$

$Z_{10} = \{0,1,2,3,4,5,6,7,8,9\} \qquad Z_{10}^* = \{1,3,7,9\}$

Note. For all $p \in P$, the multiplicative group is

$$Z_p^* = Z_p \backslash \{0\} = \{1,2,3,\dots,p-1\}$$

Note. **G**roup Z_n^* with operation $\cdot\ (mod\ n)$ is always Abelian, as

$$a \cdot b = b \cdot a\ (mod\ n)$$

for all $a, b \in Z_n^*$.

Example. Let us check the group properties for Z_9^*:

Multiplication table for $\mathbb{Z}_9^*$

$\times$ mod 9	**1**	**2**	**4**	**5**	**7**	**8**
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

$1^{-1} = 1$
$2^{-1} = 5$, $5^{-1} = 2$
$4^{-1} = 7$, $7^{-1} = 4$
$8^{-1} = 8$

- closed under $\times\ (mod\ 9)$
- associativity: $a \times (b \times c) = (a \times b) \times c\ (mod\ 9)$
- identity element 1 exists
- every element has a multiplicative inverse
- Abelian group:

$$a \times b = b \times a\ (mod\ 9)$$

Definition. A group $(G,\circ)$ is *finite* if it has a finite number of elements.
The *order of group* G (or *cardinality*) is denoted by $|G|$.

- All groups $Z_n$and Z_n^* are finite.
- The order $|Z_n|$ of Z_n is n.
- The order $|Z_n^*|$ of Z_n^* is $\varphi(n)$.

Example. The order of $Z_9 = \{0,1,2,3,4,5,6,7,8\}$ is $|Z_9| = 9$.

The order of $Z_9^* = \{1,2,4,5,7,8\}$ is $|Z_9^*| = 6$. $\varphi(9) = 6$

Definition. The *order of an element* $a \in (G,\circ)$ is the smallest $k \in Z_+$ for which

$$\underbrace{a \circ a \circ \ldots \circ a}_{k} = 1$$

We denote this by $ord(a) = k$.

Example. Find the orders of the elements of $Z_9^* = \{1,2,4,5,7,8\}$.

- $ord(1) = 1$

$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16 \equiv 7$
$2^5 = 2 \cdot 7 \equiv 5$
$2^6 = 2 \cdot 5 \equiv 1$ } mod 9

$\Rightarrow ord(2) = 6$

$4^1 = 4$
$4^2 = 16 \equiv 7$
$4^3 = 4 \cdot 7 \equiv 1$ } mod 9

$\Rightarrow ord(4) = 3$

Similarly,
$ord(5) = 6$
$ord(7) = 3$
$ord(8) = 2$

Definitions.

- Let $a \in G$. If $ord(a) = |G|$, then a is a *generator* or a *primitive element* of G.
- If G has a primitive element, then G is a *cyclic group*.
- A primitive element of G *generates* all elements of G.

Example. Z_9^* has two primitive elements: both 2 and 5 generate all elements of group Z_9^*. Hence Z_9^* is a cyclic group.

$5^1 = 5$
$5^2 = 25 \equiv 7$
$5^3 \equiv 5 \cdot 7 \equiv 8$
$5^4 \equiv 5 \cdot 8 \equiv 4$
$5^5 \equiv 5 \cdot 4 \equiv 2$
$5^6 \equiv 5 \cdot 2 \equiv 1$ } (mod 9)

- powers of 5 generate all elements of $\mathbb{Z}_9^*$
  → 5 is a generator
  ($ord(5) = 6 = |\mathbb{Z}_9^*|$)
  → $\mathbb{Z}_9^*$ is cyclic

Theorems on Cyclic Groups

Theorem 8.2.2 *For every prime p, $(\mathbb{Z}_p^*, \cdot)$ is an abelian finite cyclic group.*

Theorem 8.2.3
Let G be a finite group. Then for every $a \in G$ it holds that:

1. $a^{|G|} = 1$
2. *ord(a) divides $|G|$*

Theorem 8.2.4 *Let G be a finite cyclic group. Then it holds that*
1. *The number of primitive elements of G is $\Phi(|G|)$.*
2. *If $|G|$ is prime, then all elements $a \neq 1 \in G$ are primitive.*

Notes.

- Theorem 8.2.3.2 helps in finding primitive elements (f.ex. for the DHKE setup).
- The number of primitive elements in group Z_n^* is $\varphi(\varphi(n))$.
- The number of primitive elements in group Z_p^* is $\varphi(p-1)$.
- For groups Z_p^*, the order $|Z_p^*| = p - 1$, which is an even number. Hence the condition of Theorem 8.2.4.2 never holds for groups Z_p^*.

Z_9^* has $\varphi(\varphi(9))$ primitive elements

Example. (for Theorem 8.2.3.2):
Order of Z_9^* is 6, and Orders of the elements of Z_9^* are: 1,2,3,6. They are all factors of $|Z_9^*| = 6$.

$\varphi(9) = 6$ and $\varphi(6) = 2$

Example. (for Theorem 8.2.4.1):
Z_9^* has order 6 and $\varphi(6) = (2-1)(3-1) = 2$. Hence, $\varphi(\varphi(9)) = 2$ and there are 2 primitive elements in Z_9^*. (Namely 2 and 5, as we learned in a previous example.)

Example. a) Is 2 a primitive element of Z_{23}^*?

b) Is 5 a primitive element of Z_{233}^*?

a) $p = 23 \in \mathbb{P} \Rightarrow |\mathbb{Z}_{23}^*| = 22$

Divisors of 22 : 1, 2, 11, 22

$\Rightarrow$ we check if $2^k \equiv 1 \pmod{23}$ for $k = 1, 2, 11, 22$:

$2^1 = 2$
$2^2 = 4$
$2^{11} = 2048 \equiv 1$ $\pmod{23}$

Thus, $\text{ord}(2) = 11$ $(\neq 22)$ and hence 2 is not primitive in $\mathbb{Z}_{23}^*$.

b) $233 \in \mathbb{P}$, so $|\mathbb{Z}_{233}^*| = 232$

Divisors of 232:
1, 2, 4, 8, 29, 58, 116, 232

$\Rightarrow$ we check if $5^k \equiv 1 \pmod{233}$ for $k = 1, 2, 4, \ldots$

$5^1 = 5$
$5^2 = 25$
$5^4 = 159$
$5^8 = 117$
$5^{29} = 12$
$5^{58} = 144$
$5^{116} = 232$
$5^{232} = 1$
mod 233

$\Rightarrow \text{ord}(5) = 232$ and 5 is primitive in $\mathbb{Z}_{233}^*$

The Discrete Logarithm Problem in Z_p^*

Definition. Given Z_p^*, a primitive element $\alpha \in Z_p^*$ and another element $\beta \in Z_p^*$, the Discrete Logarithm problem (DLP) is the problem of finding $x \in \{1, \dots, p-1\}$ such that

$$\alpha^x = \beta \ (mod\ p)$$

Here x is the discrete logarithm of β to the base α,

$$x = \log_\alpha \beta \ \ (mod\ p)$$

For large values of $\alpha,\ \beta$ and p, solving the DLP is computationally infeasible, whereas finding $\alpha^x \ (mod\ p)$ is easy given α, x and p. Therefore, the DLP is considered to be a one-way function.

Example. Consider the multiplicative group Z_{47}^* with primitive element $\alpha = 5$. For $\beta = 41$, the DLP is: Find $x \in \{1,2, \dots ,46\}$ such that

$$5^x \equiv 41 \ \ (mod\ 47)$$

By brute force, we can try $5^1,\ 5^2,\ 5^3 \dots \ \ (mod\ 47)$ and find that

$$5^{15} \equiv 41\ (mod\ 47)$$

Hence, $x = 15$.

Generalized Discrete Logarithm Problem

The DLP is not restricted to Z_p^*, but can be defined over any cyclic group. This makes the DLP very useful in cryptography.

Definition. Given a finite cyclic group G with the group operation $\circ$ and order n, a primitive element $\alpha \in G$ and another element $\beta \in G$, the Discrete logarithm problem is finding the integer x such that

$$\beta = \underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_{x\ times} = \alpha^x$$

Example. $(Z_{11}, +)$ is an additive group of integers modulo prime 11. It has a primitive element $\alpha = 2$:

i	1	2	3	4	5	6	7	8	9	10	11
$i\alpha$	2	4	6	8	10	1	3	5	7	9	0

Here we use notation $\underbrace{2 + 2 + \cdots + 2}_{x} = x \cdot 2$.

Let us solve the DLP in $(Z_{11}, +)$ for $a = 2,\ b = 5$. We must solve for x in

$$x \cdot 2 \equiv 5\ (mod\ 11)$$

To find x, we just need to find the inverse of 2:

$$x = 5 \cdot 2^{-1}\ (mod\ 11)$$

Using the EEA, we can easily find that $2^{-1} \equiv 6\ (mod\ 11)$ and therefore

$$x = 5 \cdot 6 \equiv 8\ (mod\ 11)$$

As demonstrated in the previous example, the DLP is not difficult to solve in every cyclic group. It turns out that the DLP is computationally easy to solve in *all* additive groups $(Z_p, +)$. Obviously, we can only use groups for which the DLP is hard in public-key cryptosystems. The most popular cyclic groups for which the DLP is used in cryptography are multiplicative groups $(Z_p^*,\ \cdot\ )$ of prime fields Z_p, or their subgroups, and Elliptic Curve cyclic groups.

The Diffie-Hellman Problem

Definition. Let G be a finite cyclic group of order n. Then the Diffie-Hellman Problem (DHP) is the following: Given a primitive element $\alpha \in G$ and two elements $A = \alpha^a \in G$ and $B = \alpha^b \in G$, find the element $\alpha^{ab} \in G$.

Alice		**Bob**
Choose private key $a \in \{2, \dots, p-2\}$		Choose private key $b \in \{2, \dots, p-2\}$
Compute public key $A = \alpha^a \ (mod\ p)$		Compute public key $B = \alpha^b \ (mod\ p)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
Compute shared key $k_{AB} = B^a \ (mod\ p)$		Compute shared key $k_{AB} = A^b \ (mod\ p)$

It is *assumed* that the only way to solve the DHP is to solve the underlying DLP. As the DLP is computationally infeasible for large enough n, also the DHP is considered computationally secure. However, it is still possible that there is another, easier way to solve the DHP.