3. Number theory

3.1. Divisibility

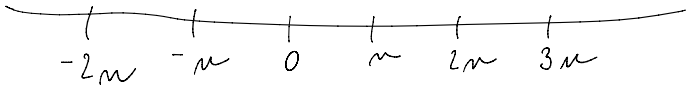
$\mathbb{Z}$ - the set of all integers

$\mathbb{N}$ - the set of all natural numbers

Definition: Let n, m be integers. We say that n devides m (in symbols $n \mid m$) if there is $k \in \mathbb{Z}$ such that

$$m = kn$$

- Observe:
  - $n \mid m \Rightarrow |n| \leq |m|$
  - $n \mid m \Leftrightarrow |n| \mid |m|$
- $n \mid m \Longleftrightarrow m \in \{kn \mid k \in \mathbb{Z}\}$



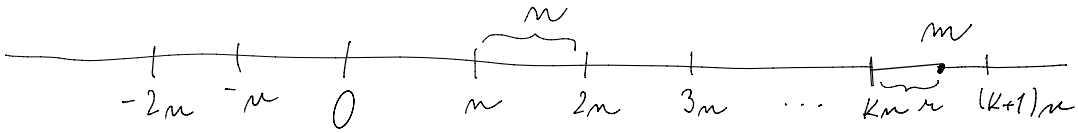
Theorem (DIVISION)

For each $n \in \mathbb{N}$ and $m \in \mathbb{Z}$ there is a unique $K \in \mathbb{Z}$ and $r \in \{0, 1, \dots, n-1\}$ such that

$$m = Kn + r$$

(K: quotient, r: remainder)

Proof: See the picture



$r \in [0, n)$

□

Definition: Suppose $a, b \in \mathbb{Z} \setminus \{0\}$.
A number $d \in \mathbb{N}$ is called the greatest common divisor of a and b if the following two conditions are satisfied:

(1) $d \mid a$ and $d \mid b$

(2) If $d' \in \mathbb{N}$ devides a and b then $d' \mid d$

Notation $d = \gcd(a,b)$

Observation
- $\gcd(a,b) = \gcd(|a|,|b|)$
- If $a, b > 0$
  $a \mid b \implies \gcd(a,b) = a$
- $\gcd(0,a) = a$

Example: $\gcd(12,18) = 6$

- It is not apriori clear that gcd exists.
  A necessary condition for d being $\gcd(a,b)$

is that d is the greates element (in the standard order) of all positive common divisors of a and b.
But is it sufficient? Is the greatest element of the set of all divisors divisable by each element of this set?

Theorem (Bézout Theorem)

For any $a, b \in \mathbb{Z} \setminus \{0\}$ there are $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a,b)$$

Proof: Put

$$S_{a,b} = \{xa + yb \mid x, y \in \mathbb{Z}\}$$

Observe that
- $S_{a,b}$ is closed under addition

Observe that

- $S_{a,b}$ is closed under addition
- $S_{a,b}$ is closed under multiplying by integer
- $S_{a,b}$ contains $\{a, b\}$.

Put

$$n = \min\{z \in S_{a,b} \mid z > 0\}$$

Such minimum must exist.

Write

$$n = x_0 a + y_0 b \qquad x_0, y_0 \text{ are integers}$$

We prove that $n = \gcd(a,b)$

$n \mid a$: $\quad a = kn + r$, k integer, $r \in \{0, \dots, n-1\}$

Clearly $\quad r = a - kn \in S_{a,b}$

So $\quad r = 0$ because otherwise we have a contradiction with minimality of n.

Hence, $\quad r = 0$ and so $n \mid a$. For the same reason $n \mid b$.

Finally, suppose $d' \mid a$ and $d' \mid b \Rightarrow d' \mid x_0 a + y_0 b = n$.

So $\quad n = \gcd(a,b)$ □

Corollary $\quad \gcd(a,b) = \max\{t \mid t \mid a \text{ and } t \mid b\}$.

How to find $\gcd(a,b)$ for a, b large.

Proposition Let $0 < a < b$ be natural numbers.
Let

$$b = Ka + r, \quad K \in \mathbb{N} \text{ and } r \in \{0, 1, \dots, n-1\}$$

then $\gcd(a,b) = \gcd(a,r)$

Proof: $\ell \mid a, b \iff \ell \mid a, r$

So the sets of common divisors of $\{a,b\}$ and $\{a,r\}$ are same. Therefore by corollary

$$\gcd(a,b) = \gcd(a,r)$$

□

Idea of Euclid algorithm $a < b$

$$\gcd(a,b) = \gcd(a,r) = \gcd(r,r')$$

(r: smaller than a; $a = kr + r'$; $r' < r$)

Once we have to reach remainder is zero. We then use

$$\gcd(0,m) = m$$

Euclid algorithm

$0 < a < b$ integers

$$b = k_0 a + r_0 \qquad r_0 < a$$
$$a = k_1 r_0 + r_1 \qquad r_1 < r_0$$
$$r_0 = k_2 r_1 + r_2$$
$$\vdots$$
$$r_j = k_{j+2} r_{j+1} + r_{j+2}$$

$$\gcd(a,b) = \gcd(a,r_0) = \gcd(r_0,r_1) = \cdots = \gcd(r_{j+1},0) = r_{j+1}$$

after finitely many steps we have

$$r_{j+2} = 0$$

$$\gcd(a, b) = r_{j+1}$$

Example $\gcd(432, 234)$

$$432 = 1 \cdot 234 + 198$$

$$234 = 1 \cdot 198 + 36$$

$$198 = 5 \cdot 36 + 18$$

$$36 = 2 \cdot 18 + 0$$

$$\gcd(432, 234) = \gcd(0, 18) = 18$$

3.2. Linear Diophantine equation

Example: Find all $x, y \in \mathbb{Z}$ such that

$$432x + 234y = 18$$

Solution: run Euclid algorithm backwards

$$18 = 198 - 5 \cdot 36 = 198 - 5 \cdot (234 - 198) =$$

$$= 6 \cdot 198 - 5 \cdot 234 = 6 \cdot (432 - 234) - 5 \cdot 234$$

$$= 6 \cdot 432 - 11 \cdot 234$$

$$x = 6, \quad y = -11.$$

Example: Find $x, y \in \mathbb{Z}$ such that

$$16x - 12y = 0$$

Solution: divide by 4

$$4x - 3y = 0$$

Suppose $x, y \neq 0$

Suppose $x, y \neq 0$

$$\frac{y}{x} = \frac{4}{3}$$

So $y = 4k$ $\quad k \in \mathbb{Z}$

$x = 3k$

This can be generalized:

Theorem Let a, b be non-zero integers. The equation

$$ax + by = 0$$

has infinitely many solutions given by

$$x = k\frac{b}{\gcd(a,b)} \qquad y = -k\frac{a}{\gcd(a,b)} \quad ; k \in \mathbb{Z}$$

Proof: $x, y \neq 0$

$$\frac{y}{x} = -\frac{b}{a}$$

$\downarrow$ cancel

$$\frac{y}{x} = \frac{-b/\gcd(a,b)}{a/\gcd(a,b)}$$

$$\Rightarrow y = -k\frac{b}{\gcd(a,b)} \qquad k \in \mathbb{Z}$$

$$x = k\frac{a}{\gcd(a,b)}$$

□

Theorem Let a, b, c be non-zero integers. Then there exists $x, y \in \mathbb{Z}$ such that

$$ax + by = c$$

if and only if

$$\gcd(a,b) \mid c.$$

Proof: If $ax+by=c \Rightarrow \gcd(a,b) \mid c$

For the converse

Suppose that $c = k \cdot \gcd(a,b)$ for some $k \in \mathbb{Z}$

By Bézout theorem there are $x_0, y_0 \in \mathbb{Z}$ such that

$$ax_0 + by_0 = \gcd(a,b) \quad /k$$

$$ax + by = c$$

for $x = kx_0$

$y = ky_0$.

□

Example $24x + 105y = 33$

Solution: find $\gcd(24, 105)$

Euclid:

$$105 = 4 \cdot 24 + 9$$

$$24 = 2 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3$$

$\gcd(24, 105) = 3$

$3 \mid 33$ ✓

First find solution to

$$24x + 105y = 3$$

Backwards:

$$3 = 9 - 6 = 3 \cdot 9 - 24 =$$

$$= 3 \cdot (105 - 4 \cdot 24) - 24 =$$

$$= 3 \cdot 105 - 13 \cdot 24 \quad /11$$

$$31 = 33 \cdot 105 - 143 \cdot 24$$

$x = 33$

$y = 143$

Theorem Let a, b, c be non-zero integers such that $\gcd(a,b) \mid c$.

Suppose that $x_1, y_1 \in \mathbb{Z}$ is some solution of the equation

$$ax + by = c$$

Then all solutions are of the form

$$x = x_1 + k\frac{b}{\gcd(a,b)} \quad y = y_1 - k\frac{a}{\gcd(a,b)} \quad ; \quad k \in \mathbb{Z}$$

Proof: Let $ax + by = c$ $x, y \in \mathbb{Z}$

as $ax_1 + by_1 = c$

we have

$$a(x - x_1) + b(y - y_1) = 0$$

$$\Rightarrow \quad x - x_1 = k\frac{b}{\gcd(a,b)} \qquad k \in \mathbb{Z}$$

$$y - y_1 = -k\frac{a}{\gcd(a,b)}$$

□

3.3. Positional number system

- We are using decimal system

e.g. $123 = 1 \cdot 10^2 + 2 \cdot 10 + 3 \cdot 10^0$

$= (123)_{10}$

Instead of 10 we can use other base $q > 1, 2$.

$$n = (a_k a_{k-1} \cdots a_1 a_0)_q$$

$$= a_k q^k + a_{k-1} q^{k-1} + \cdots + a_1 q + a_0$$

where $k \in \mathbb{N} \cup \{0\}$

$a_i \in \{0, 1, \cdots, q-1\}$

q is called *base*

$a_K, a_{K-1}, \dots, a_0$ are called *digits*

Example Write $n = 174$ in base $q = 3$

Solution: powers of 3

$3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 9 \quad 3^3 = 27 \quad 3^4 = 81 \quad 3^5 = 273, \dots$

↓ enough

$174 = 2 \cdot 81 + 12 \qquad a_4 = 2$

$12 = 0 \cdot 27 + 12 \qquad a_3 = 0$

$12 = 1 \cdot 9 + 3 \qquad a_2 = 1$

$3 = 1 \cdot 3 + 0 \qquad a_1 = 1$

$147 = (20110)_3 \qquad a_0 = 0$

Theorem: Consider $q \in \mathbb{N} \setminus \{1\}$. Then every number $n \in \mathbb{N}$ can be uniquely expressed

$$a = \sum_{i=0}^{K} a_K q^K = a_K q^K + a_{K-1} q^{K-1} + \dots + a_0 q^0$$

where $a_i \in \{0, 1, \dots, q-1\}$, $K \in \mathbb{N} \cup \{0\}$

Proof: Existence: by the algorithm

Uniqueness: Suppose

$$n = a_K q^K + a_{K-1} q^{K-1} + \dots + a_0$$

$$= b_\ell q^\ell + b_{\ell-1} q^{\ell-1} + \dots + b_0$$

$a_K, b_\ell \neq 0$

First we prove $K = \ell$.

By contradiction assume $\ell > K$ $(a_K, b_\ell \neq 0)$

$$a = \sum_{i=0}^{K} a_i q^i \leq \sum_{i=0}^{K} (q-1) q^i = (q-1) \sum_{i=0}^{K} q^i$$

By contradiction assume $l > K$ (a_K, a_{K+1})

$$a = \sum_{i=0}^{K} a_i q^i \le \sum_{i=0}^{K} (q-1) q^i = (q-1) \sum_{i=0}^{K} q^i$$

$$= (q-1) \frac{q^{K+1} - 1}{q-1} = q^{K+1} - 1$$

However, $q^{K+1} - 1 < q^l \le \sum_{i=0}^{l} b_i q^i = a$

contradiction

So $l = K$.

Let us show now that $a_K = b_K$

Similar estimation: Let $b_K > a_K$

$$a \le a_K q^K + q^K - 1 = (a_K + 1) q^K - 1 \le b_K q^K - 1 < a$$

again contradiction.

3.4. Congruence

Definition Two numbers $a, b \in \mathbb{Z}$ are called **relatively prime**

if $gcd(a, b) = 1$

In symbols, $a \perp b$

Euclid lemma Let a, b, c be non-zero integers such that $a \perp b$. Then

$$a \mid bc \Rightarrow a \mid c$$

Proof: $a \mid bc \Rightarrow \exists d \in \mathbb{Z}$ with $bc = da$

$a \perp b \xrightarrow{\text{Bézout}} ax + by = 1$ for some $x, y \in \mathbb{Z}$.

$\downarrow$ multiply by c

$$c = acx + bcy = acx + ady =$$

$$c = acx + bcy = acx + ady =$$
$$= a(cx + dy)$$

$$\Rightarrow a \mid c.$$

□

Definition Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

We say that *a is congruent to b modulo n* if $n \mid (a-b)$

In symbols, $\boxed{a \equiv b \pmod{n}}$

Observation For a, b integers the following statements are equivalent.

(1) $a \equiv b \pmod{n}$

(2) a and b have the same remainder when dividing by n

(3) $a = b + kn$ for some $k \in \mathbb{Z}$

Proof (1) $\Leftrightarrow$ (3) obvious

(1) $\Rightarrow$ (2) Write

$$a = kn + r_1 \qquad 0 \le r_1, r_2 \le n-1$$
$$b = ln + r_2$$

WLOG assume $r_1 \ge r_2$

$$a - b = (k-l)n + (r_1 - r_2)$$
$$0 \le \quad \le n-1$$

$a - b$ has zero remainder $\Rightarrow r_1 - r_2 = 0$.

Theorem (Properties of congruence)

Let $a, b, c, d \in \mathbb{Z}$; $n, k \in \mathbb{N}$

Then

(1) $a \equiv a \pmod n$ [congruence is reflexive]

(2) $a \equiv b \pmod n \iff b \equiv a \pmod n$

[congruence is symmetric]

(3) $[a \equiv b \pmod n \wedge b \equiv c \pmod n] \Rightarrow a \equiv c \pmod n$

[congruence is transitive]

$\equiv$ is equivalence on $\mathbb{Z}$

(5) $a \equiv b \pmod n \Rightarrow a + c \equiv b + c \pmod n$

(6) $a \equiv b \pmod n \Rightarrow ac \equiv bc \pmod n$

(7) $\left.\begin{array}{l} a \equiv b \pmod n \\ \text{and} \quad c \equiv d \pmod n \end{array}\right\} \Rightarrow ac \equiv bc \pmod n$

(8) $a \equiv b \pmod n \Rightarrow a^k \equiv b^k \pmod n$

(9) $ac \equiv bc \pmod n \wedge c \perp n \Rightarrow a \equiv b \pmod n$

(10) $a \equiv b \pmod n \iff ak \equiv bk \pmod{kn}$

Proof : tutorial + homework

(7) $a - b = kn$

$c - d = ln$

Then

$$ac = (b + kn)(d + ln)$$
$$= bd + knd + bln + kln^2$$
$$= bd + n(kd + bl + kln)$$

($kd + bl + kln$: integer)

(8) It follows from recurrent application of (7)

integer

(8) It follows from recurrent application of (7) for $a=c$ $b=d$

alternative: $a \equiv b \pmod n$ i.e. $n \mid a-b$

$$a^k - b^k = (a-b)\underbrace{\left[a^k + a^{k-1}b + a^{k-2}b + a^{k-3}b^2 + \cdots + b^{k-1}\right]}_{\text{integer}}$$

So $n \mid a-b \Rightarrow n \mid a^k - b^k$

- $a \equiv a_1 \pmod n$, $b \equiv b_1 \pmod n$ $\Rightarrow a+b \equiv (a_1+b_1) \pmod n$

$a = a_1 + kn$, $b = b_1 + ln$ $\Rightarrow a+b = (a_1+b_1) + (k+l)n$.

Application to divisibility criteria

Example: $n = (a_k a_{k-1} \cdots a_1 a_0)_{10}$

Then $n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 3$

basic powers: $1 \equiv 1 \pmod 3$

$10 \equiv 1 \pmod 3$

by (8) $10^k \equiv 1^k \pmod 3$

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_0$$
$$\equiv (a_k \cdot 1 + a_{k-1} \cdot 1 + \cdots + a_0 \cdot 1) \pmod 3$$

Therefore $3 \mid n \Leftrightarrow 3$ divides the sum of its decimal digits.

Example Find criterion for divisibility by 11

Solution: $10 \equiv -1 \pmod{11}$

$10^2 \equiv (-1)^2 \pmod{11}$

$$10^i \equiv (-1)^i \pmod{11}$$

So

$$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^K a_K \pmod{11}$$

e.g. $11 \mid 2345 \iff 11 \mid 5-4+3-2 = 2$ - no

- Solving equations with congruences

Theorem: Let a, b be integers and n natural number. Then there is an integer x solving equation

$$ax \equiv b \pmod{n}$$

if and only if

$$\gcd(a,n) \mid b$$

Proof: $ax \equiv b \pmod{n}$

$\iff$ $b = ax + kn$ for some $k \in \mathbb{Z}$

By the previous theorem this equation has solution

$\iff$ $\gcd(a,n) \mid b$.

□

Exercise: Find all $x \in \mathbb{Z}$ such that

$$29x \equiv 1 \pmod{17}$$

Solution based on Euclid algorithm:

$$1 = 29x + k \cdot 17$$

$$29 = 1 \cdot 17 + 12$$

$$17 = 1 \cdot 12 + 5$$

$$12 = 2 \cdot 5 + 2$$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$ $\quad \gcd(29,17) = \gcd(1,0) = 1$

$1 = 5 - 2 \cdot 2 = 5 - 2(12 - 2 \cdot 5) =$

$= -2 \cdot 12 + 5 \cdot 5 = 5 \cdot 17 - 7 \cdot 12 -$

$= -7 \cdot 29 + 12 \cdot 17$

$x = -7$

all solutions: $x = -7 + 17k \mid k \in \mathbb{Z}$

(see general solution of Diophantic equation above.

Solution based on rules

$29x \equiv 1 \quad | -17x \equiv 0$

$12x \equiv 1 \quad | + 0 \equiv 17$

$12x = 18 \quad | : 6$ (1) $\gcd(6,17) = 1$

$2x \equiv 3 \quad | + 0 \equiv 17$

$2x \equiv 20$ → (1) $\gcd(2,17) = 1$

$x \equiv 10$

3.5 Primes

Definition A prime number is a number $p \in \mathbb{N}$ $p > 1$ that has exactly two positive divisors, namely 1 and p.
a number that is not prime is called a
a composite number

Theorem Consider $p \in \mathbb{N}$, $p > 1$. Then

p is prime $\Leftrightarrow [p \mid bc \Rightarrow p \mid b$ or $p \mid c]$

p is prime $\Leftrightarrow$ [$p \mid bc \Rightarrow p \mid b$ or $p \mid c$]

Proof: $\Rightarrow$

Suppose p is prime $p \mid bc$.
If p does not devide b. The $p \perp b$ as p is prime
By Euclid lemma we get $p \mid c$.

$\Leftarrow$ Suppose $p = d_1 d_2$, $0 \leq d_1, d_2$. We have $d_1, d_2 \leq p$.

$p \mid d_1 d_2 \underset{\text{assumption}}{\Rightarrow}$ $p \mid d_1$ or $p \mid d_2$

Suppose $p \mid d_1 \Rightarrow p \leq d_1$. This means that $d_1 = p$.

□

Fundamental theorem of arithmetic

Every $n \in \mathbb{N}$, $n > 1$ can be written as a product of prime numbers. This prime factorization is unique up to the order of factors

Proof:

Induction: Suppose that n is a composite number such that prime factorization exists for all numbers smaller than n.

$$n = n_1 n_2 \qquad 1 < n_1, n_2 < n$$

By induction n_1 and n_2 can be expressed as products of prime numbers and the same holds for n.

Uniqueness: by contradiction

Suppose that n is the smallest number for which the prime factorization is not unique.

$$n = p_1 p_2 \cdots p_k \quad \left.\begin{matrix} \\ \\ \end{matrix}\right\} \text{two different prime factorizations}$$
$$n = q_1 q_2 \cdots q_\ell$$

Applying theorem above we have that

$$p_1 \mid q_j \text{ for some } j \Rightarrow p_1 = q_j$$

But this means that

$$m = \frac{n}{p_1} = \frac{n}{q_j}$$

has two different prime factorizations $\Rightarrow$ a contradiction

□

Example Factorize 242

$$242 = 2 \cdot 121 = 2 \cdot 11 \cdot 11$$

Theorem There are infinitely many prime numbers.

Proof: By contradiction, assume that

$$p_1, p_2, \cdots, p_k$$

are the only prime numbers

Consider

$$n = p_1 p_2 \cdots p_k + 1 = \underbrace{q_1 \cdots q_\ell}_{\text{prime number}}$$

prime number factorization

But $p_i \equiv 1 \pmod{n}$

for $p_i \neq q_j \ \forall i,j \Rightarrow q_j$'s are not in the list – contradiction.

For p prime and $a \in \mathbb{N}$

$a \perp p \Leftrightarrow p$ does not divide a.

Fermat's little theorem

Let p be prime, $a \in \mathbb{N}$, $a \perp p$. Then

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

Proof: First step is to show that

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

binomial theorem

$$(x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j}$$

We claim that

$$p \mid \binom{p}{j} \quad \text{unless} \quad j=0 \text{ or } j=p$$

$$\binom{p}{j} = \frac{p(p-1)(p-2)\cdots(p-j+1)}{j!}$$

- $j! \mid p(p-1)\cdots(p-j+1)$ (*)

- p cannot divide $j!$. Indeed from Euclid lemma the p would divide some $j-k < p$.

- Now by (*) and the fact that $p \perp j!$ we obtain from Euclid lemma again that

$p \nmid j! \Rightarrow$ $\quad j! \mid (p-1)(p-2)\cdots 1$

Therefore $\quad p \mid \binom{p}{j}$

This shows that

$$(x+y)^p \equiv x^p + y^p \pmod p$$

By induction

$$(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod p$$

Write $\quad a = 1+1+\cdots+1$

$$a^p = (1+1+\cdots+1)^p \equiv 1^p + 1^p + \cdots + 1^p \pmod p =$$

$$= 1+1+\cdots+1 \pmod n \equiv a \pmod p$$

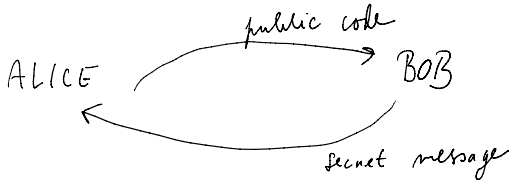
Hence $\quad a^p \equiv a \pmod p$

i.e. $\quad p \mid a^p - a = a(a^{p-1} - 1)$

$p \nmid a \overset{\text{Euclid}}{\Rightarrow} p \mid a^{p-1} - 1.$ $\square$

3.5. RSA encoding

RIVEST, SHAMIR, ADLEMAN (1977)



ALICE: Choose randomly large primes p, q and compute $n = pq$

ALICE: Choose randomly large primes p, q
and compute $n = pq$
Denote $\phi(n) = (p-1)(q-1)$

choose some number

$i \in \{2, 3, \dots, \phi(n)-1\}$

such that $i \perp \phi(n)$

public key : (n, i)

She computes for herself a number j solving equation

$ij - k\phi(n) = 1$ (Bézout theorem)

In other words, $ij \equiv 1 \pmod{\phi(n)}$ (Euclid algorithm)

Alice $\xrightarrow{(n,i)}$ Bob

Alice

Bob - message x - integer

$0 < x < n$

decoding

$y = x^i \bmod(n)$ (= remainder)

$x = y^j \bmod(n)$

↑ encoding x

OK by the following theorem

Theorem: Let p, q be prime numbers.
Let $n = pq$ $\phi(n) = (p-1)(q-1)$
Let $i, j \in \mathbb{N}$ satisfy

$ij \equiv 1 \pmod{\phi(n)}$

Then

$x^{ij} \equiv x \pmod{n}$ $\forall$ integer x

Proof

- $ij \equiv 1 \bmod(\phi(n)) \Leftrightarrow ij = k\phi(n) + 1 = k(p-1)(q-1)+1 \qquad k \in \mathbb{Z}$
- $a^{ij} \equiv a \pmod{n} \Leftrightarrow a^{ij} \equiv a \pmod{p}$
  and $a^{ij} \equiv a \pmod{q}$

argument: denote $a = a^{ij}$

$\Rightarrow$

$a - a = npq \qquad n \in \mathbb{Z}$

$\Rightarrow a - a = (np)q = (nq)p$

so $a \equiv a \pmod{p}$ and $a \equiv a \pmod{q}$

$\Leftarrow$

$a - a = np \qquad n, l \in \mathbb{Z}$

$a - a = lq$

so $a - a$ has p, q in prime number decomposition

$\Rightarrow ab = a(pq) \qquad l \in \mathbb{Z}$

We shall prove that

$$a^{ij} \equiv a \pmod{p}$$

Suppose that $a \perp p$. By the little Fermat theorem

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

power $k(p-1)(q-1)$

$$a^{k(p-1)(q-1)} \equiv \underbrace{1^{k(q-1)}}_{=1} \pmod{p}$$

multiply by a

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{p}$$

$$a^{ij} \equiv a \pmod{p}.$$

If $a \not\perp p$ then $a = sp, \ s \in \mathbb{Z}$

so $a \equiv 0 \pmod{p}$ as well as

$a^{ij} \equiv 0 \pmod{p}$

□

Example

Alice $p = 11$, $q = 13$, $n = pq = 143$

$\phi(n) = 10 \cdot 12 = 120$

$i = 17$ (it is prime)

Find j such that

$$17j - K \cdot 120 = 1$$

$120 = 7 \cdot 17 + 1$

$1 = 120 - 7 \cdot 17 = -16 \cdot 120 + 113 \cdot 17$

So $j = 113$

Public code $n = 143$

$i = 17$

Bob wants to send $u = 69$

Encryption needs to compute $69^{17} \bmod 143$

all mod 143

$69 \equiv 69$

$69^2 = 4761 \equiv 42$

$69^4 \equiv 42^2 \equiv 48$

$69^8 \equiv 48^2 \equiv 46$

$69^{16} \equiv 16^2 \equiv 113$

$69^{17} = 69^{16} \cdot 69 \equiv 113 \cdot 69 \equiv 75$

So $y = 75$ ⟶ send to Alice

Alice: needs to compute $75^{113} \bmod 143$

$75^1 \equiv 75$

$75^2 \equiv 48$

$75^4 \equiv 48^2 \equiv 16$

$75^8 \equiv 16^2 \equiv 113$

$75^{16} \equiv 113^2 \equiv 123$

$$75^8 \equiv 16^2 \equiv 113$$
$$75^{16} \equiv 113^2 \equiv 42$$
$$75^{32} \equiv 42^2 \equiv 48$$
$$75^{64} \equiv 48^2 \equiv 46$$

$113 = 64 + 32 + 16 + 1 \quad (= (1110001)_2)$

$$75^{-113} = 75^{64} \cdot 75^{32} \cdot 75^{16} \cdot 75 \equiv 46 \cdot 48 \cdot 42 \cdot 75 \equiv 69$$