GCD and Chinese Remainder Theorem

Amitava Bhattacharya

TIFR, Mumbai

2 Jan 2021

Mumbai Math Circle is a collaboration of TIFR and St Xaviers College Mumbai.

Designed by *Sukant Saran* (www.sukantsaran.in)

There are infinitely many prime numbers

There are infinitely many prime numbers
Euclid's Argument:
Let $L = \{p_1, p_2, \ldots, p_k\}$ be a finite list of primes.

There are infinitely many prime numbers
Euclid's Argument:
Let $L = \{p_1, p_2, \ldots, p_k\}$ be a finite list of primes.

$$N = p_1 p_2 p_3 \ldots p_k + 1$$

There are infinitely many prime numbers
Euclid's Argument:
Let $L = \{p_1, p_2, \ldots, p_k\}$ be a finite list of primes.

$$N = p_1 p_2 p_3 \ldots p_k + 1$$

This number cannot be divided by any or the primes in the list L.

There are infinitely many prime numbers
Euclid's Argument:
Let $L = \{p_1, p_2, \ldots, p_k\}$ be a finite list of primes.

$$N = p_1 p_2 p_3 \ldots p_k + 1$$

This number cannot be divided by any or the primes in the list L.
This implies either N is a prime itself or it is divisible by a prime not in the list.

There are infinitely many prime numbers
Euclid's Argument:
Let $L = \{p_1, p_2, \ldots, p_k\}$ be a finite list of primes.

$$N = p_1 p_2 p_3 \ldots p_k + 1$$

This number cannot be divided by any or the primes in the list L.
This implies either N is a prime itself or it is divisible by a prime not in the list.
This implies there is at least 1 more prime.

Fermat number

For $n = \{0, 1, 2, \ldots\}$

$$F(n) := 2^{2^n} + 1$$

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, \ldots$$

Fermat number

For $n = \{0, 1, 2, \ldots\}$

$$F(n) := 2^{2^n} + 1$$

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, \ldots$$

Any two Fermat numbers are relatively prime.
It means $gcd\ (F(i), F(j)) = 1$ if $i \neq j$.

Fermat number

For $n = \{0, 1, 2, \ldots\}$

$$F(n) := 2^{2^n} + 1$$

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, \ldots$$

Any two Fermat numbers are relatively prime.
It means $gcd\ (F(i), F(j)) = 1$ if $i \neq j$.
$gcd\ (a, b) = gcd\ (b, a) = gcd\ (a - b, b)$ if $a > b$

Exercise: Consider the number $2^p - 1$ where p is a prime. Show that all its prime factors are greater than p.
Exercise: Consider any polynomial $P(x)$. Show that the sequence $P(0), P(1), \ldots$ cannot be only prime numbers.

Frustenberg's proof: (Mercer's note)
Notation: All integers conguuent to $r \mod m$ is denoted by $r + m\mathbb{Z}$ and they are called AP.
Example:

$$3 + 11\mathbb{Z} = \{\dots, -30, -19, -8, 3, 14, 25, 36, \dots\}$$

For $m > 1$, set of integers not divisible (ND) by m are as

$$(1 + m\mathbb{Z}) \cup \cdots \cup ((m-1) + m\mathbb{Z}).$$

Assertion 1: Intersection of two AP's is either empty or infinite.

Assertion 1: Intersection of two AP's is either empty or infinite.
Assertion 2: Finite intersection of finite unions of sets is also a finite union of finite intersections of sets.
Example:

$$(A \cup B \cup C) \cap (D \cup E) \cap (F \cup G) = (A \cap D \cap F) \cup () \cup \dots$$

Proof: If $p_1, p_2, \dots, p_k$ is the set of all primes then

$$\{-1, 1\} = ND(p_1) \cap ND(p_2) \dots \cap ND(p_k)$$

RHS is either empty or infinite!

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots \to \infty$$

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots \to \infty$$

What about prime numbers ?

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots \to \infty$$

What about prime numbers ?

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots =?$$

We give a proof by Erdös.

Paul Erdös (Hungarian: 1913 –1996)
Erds published around 1,500 mathematical papers during his lifetime.

Suppose

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots = M$$

(p_i's are in increasing order) Then there must be a k such that

$$\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$$

Suppose

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots = M$$

(p_i's are in increasing order) Then there must be a k such that

$$\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$$

Let $P_s = p_1, p_2, \ldots, p_k$ be called small primes and
$P_b := p_{k+1}, p_{k+2}, \ldots$ be called big primes.

For any natural number N we must have

$$\sum_{i=k+1}^{\infty} \frac{N}{p}_{i} < \frac{N}{2}$$

For any natural number N we must have

$$\sum_{i=k+1}^{\infty} \frac{N}{p_{\ i}} < \frac{N}{2}$$

Let N_b be the number of integers $\leq N$ that is divisible by at least one big prime.
Let N_s be the number of integers $\leq N$, that are divisible by only small primes.
Clearly $N_b + N_s = N$.

For any natural number N we must have

$$\sum_{i=k+1}^{\infty} \frac{N}{p_{\ i}} < \frac{N}{2}$$

Let N_b be the number of integers $\leq N$ that is divisible by at least one big prime.
Let N_s be the number of integers $\leq N$, that are divisible by only small primes.
Clearly $N_b + N_s = N$.
We will show that for a suitable N, $N_s + N_b < N$, a contradiction.

$$N_b \leq \sum_{i>k} \left\lfloor \frac{N}{p}_i \right\rfloor < \frac{N}{2}$$

$$N_b \leq \sum_{i>k} \left\lfloor \frac{N}{p}_i \right\rfloor < \frac{N}{2}$$

To estimate N_s, write $n < N$ as $n = ab^2$. a squarefree part and a squared part.
Total choices number of for square free part is at most 2^k.

$$N_b \leq \sum_{i>k} \left\lfloor \frac{N}{p}_i \right\rfloor < \frac{N}{2}$$

To estimate N_s, write $n < N$ as $n = ab^2$. a squarefree part and a squared part.
Total choices number of for square free part is at most 2^k.
Total number of choices for squared part is at most $\sqrt{N}$.
This implies $N_s \leq 2^k\sqrt{N}$.

$$N_b \leq \sum_{i>k} \left\lfloor \frac{N}{p}_i \right\rfloor < \frac{N}{2}$$

To estimate N_s, write $n < N$ as $n = ab^2$. a squarefree part and a squared part.
Total choices number of for square free part is at most 2^k.
Total number of choices for squared part is at most $\sqrt{N}$.
This implies $N_s \leq 2^k\sqrt{N}$.
For contradiction find N such that $2^k\sqrt{N} < \frac{N}{2}$.

Issai Schur (1875–1941) was a Russian mathematician who worked in Germany. He was a student of the great group theorist Frobenius. Schur worked in various areas and proved many deep results in representation theory.

Issai Schur (1875–1941) was a Russian mathematician who worked in Germany. He was a student of the great group theorist Frobenius. Schur worked in various areas and proved many deep results in representation theory.

Let $P(x)$ be a non-constant polynomial with integer coefficients. Then $\{P(i) : i \in \mathbb{N}\}$ has infinitely many prime divisors.
(see Lemma 3 in https://mast.queensu.ca/~murty/poly2.pdf)

Christian Elsholtz: Prime divisors of thin sequences, Amer. Math. Monthly 119 (2012), 331–333

Let $S := \{s_1, s_2, \ldots\} \subset \mathbb{Z}$ be a sequence of integers such that

1. No integer appears more than c times.
2. S has subexponential growth i.e. $|s_n| < 2^{2^{f(n)}}$ where $\frac{f(n)}{\log_2 n} \to 0$. ($f : \mathbb{N} \to \mathbb{R}$)

Christian Elsholtz: Prime divisors of thin sequences, Amer. Math. Monthly 119 (2012), 331–333

Let $S := \{s_1, s_2, \ldots\} \subset \mathbb{Z}$ be a sequence of integers such that

1. No integer appears more than c times.
2. S has subexponential growth i.e. $|s_n| < 2^{2^{f(n)}}$ where $\frac{f(n)}{\log_2 n} \to 0$. $(f : \mathbb{N} \to \mathbb{R})$

Theorem: If a set S is "almost" injective and of sub-exponential growth (the above two conditions) then the set of prime numbers P_S that divide a member of S is infinite.

The two conditions are clearly required. Suppose the first condition does not hold. Then consider the sequence $S := \{2, 4, 4, 8, 8, 8, 8, 16, \ldots\}$.

The two conditions are clearly required. Suppose the first condition does not hold. Then consider the sequence $S := \{2, 4, 4, 8, 8, 8, 8, 16, \ldots\}$.
If the second condition does not hold then the sequence $\{2^i 3^j\}$, $i, j \in \mathbb{N}$ arranged in increasing order has $\frac{f(n)}{\log_2 n} \sim \frac{1}{2}$

Without loss of generality assume $f(n)$ is increasing.

Without loss of generality assume $f(n)$ is increasing.
Otherwise redefine it as $g(n) := \max_{i \leq n} f(n)$.
Suppose $P_S = \{p_1, p_2, \ldots, p_k\}$.
Then $s_n = \epsilon_n p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ where $\epsilon_n = \{-1, 0, +1\}$ and $\alpha_i \geq 0$
This implies

$$2^{\alpha_1+\alpha_2+\cdots\alpha_k} \leq |s_n| \leq 2^{2^{f(n)}}$$

for $s(n) \neq 0$.

$$\Rightarrow 0 \leq \alpha_i \leq \alpha_1 + \alpha_2 + \cdots \alpha_k \leq 2^{f(n)} \text{ for } 1 \leq i \leq k$$

.

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \leq (2^{f(N)} + 1)^k \leq 2^{(f(N)+1)k}.$$

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \geq \frac{N-c}{2c}$$

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \geq \frac{N-c}{2c}$$

$$\frac{N-c}{2c} \leq 2^{k(f(N)+1)}$$

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \geq \frac{N-c}{2c}$$

$$\frac{N-c}{2c} \leq 2^{k(f(N)+1)}$$

$$\log_2(N-c) - \log_2(2c) \leq k(f(N)+1) \text{ for all } N.$$

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \geq \frac{N-c}{2c}$$

$$\frac{N-c}{2c} \leq 2^{k(f(N)+1)}$$

$$\log_2(N-c) - \log_2(2c) \leq k(f(N)+1) \text{ for all } N.$$

Divide both sides by $\log_2 N$. Then LHS goes to 1 and RHS goes to 0.

$$\frac{\log_2(N-c)}{\log_2 N} \to 1 \text{ as } N \to \infty$$

and

$$\frac{f(N)}{\log_2 N} \to 0 \text{ as } N \to \infty.$$

$$\frac{\log_2(N-c)}{\log_2 N} \to 1 \text{ as } N \to \infty$$

and

$$\frac{f(N)}{\log_2 N} \to 0 \text{ as } N \to \infty.$$

This is a contradiction.

What is GCD ?

What is GCD ?
"Greatest Common Divisor"

$$GCD(4, 6) = 2, GCD(8, 0) = 8, GCD(8, 9) = 1 \ldots$$

What is GCD ?
"Greatest Common Divisor"

$$GCD(4,6) = 2, GCD(8,0) = 8, GCD(8,9) = 1 \ldots$$

$$N = \prod_p p^{\alpha_p};\ M = \prod_p p^{\beta_p}$$

What is GCD ?
"Greatest Common Divisor"

$$GCD(4,6) = 2, GCD(8,0) = 8, GCD(8,9) = 1 \ldots$$

$$N = \prod_p p^{\alpha_p};\ M = \prod_p p^{\beta_p}$$

$$GCD(N,M) = \prod_p p^{\min(\alpha_p,\beta_p)}.$$

LCM – Least Common Multiple

$$LCM(4,6) = 12, LCM(8,9) = 72, LCM(8,4) = 8, \ldots$$

$$N = \prod_p p^{\alpha_p};\ M = \prod_p p^{\beta_p}$$

$$LCM(N,M) = \prod_p p^{\max(\alpha_p,\beta_p)}.$$

LCM – Least Common Multiple

$$LCM(4,6) = 12, LCM(8,9) = 72, LCM(8,4) = 8, \dots$$

$$N = \prod_p p^{\alpha_p};\ M = \prod_p p^{\beta_p}$$

$$LCM(N,M) = \prod_p p^{\max(\alpha_p,\beta_p).}$$

Exercise: $GCD(N,M) \times LCM(M,N) = M \times N.$

How to find $GCD(N, M)$?

How to find $GCD(N, M)$?
$a \mid N$ and $a \mid M$ implies $a \mid (N + M)$ and $a \mid (N - M)$.

How to find $GCD(N, M)$?
$a \mid N$ and $a \mid M$ implies $a \mid (N + M)$ and $a \mid (N - M)$.
This generalizes to $a \mid N$ and $a \mid M$ implies $a \mid (xN + yM)$ for all $x, y \in \mathbb{Z}$.

This motivates us to consider the set

$$S(N, M) := \{xN + yM : x, y \in \mathbb{Z}\}.$$

This motivates us to consider the set

$$S(N, M) := \{xN + yM : x, y \in \mathbb{Z}\}.$$

Observations:
(A) 1f $a \in S$ then all multiples of a are also in S.

This motivates us to consider the set

$$S(N, M) := \{xN + yM : x, y \in \mathbb{Z}\}.$$

Observations:
(A) 1f $a \in S$ then all multiples of a are also in S.
(B) There is a smallest positive number d in S.

This motivates us to consider the set

$$S(N, M) := \{xN + yM : x, y \in \mathbb{Z}\}.$$

Observations:
(A) 1f $a \in S$ then all multiples of a are also in S.
(B) There is a smallest positive number d in S.
(C) $d \mid N$ and $d \mid M$

Proof of (C):

Proof of (C):

$$N = d.q + r$$

(q quotient and r remainder)

$$\begin{aligned} r &= N - dq \\ &= N - q(aN + bM) \\ &= N(1 - a) - qbM \\ &= a'N + b'M \end{aligned}$$

Proof of (C):

$$N = d.q + r$$

(q quotient and r remainder)

$$\begin{aligned} r &= N - dq \\ &= N - q(aN + bM) \\ &= N(1-a) - qbM \\ &= a'N + b'M \end{aligned}$$

This implies r is also in the set S, but r is nonnegative and strictly smaller than d.

Proof of (C):

$$N = d.q + r$$

(q quotient and r remainder)

$$\begin{aligned} r &= N - dq \\ &= N - q(aN + bM) \\ &= N(1-a) - qbM \\ &= a'N + b'M \end{aligned}$$

This implies r is also in the set S, but r is nonnegative and strictly smaller than d. This implies $r = 0$

Proof of (C):

$$N = d.q + r$$

(q quotient and r remainder)

$$\begin{aligned} r &= N - dq \\ &= N - q(aN + bM) \\ &= N(1 - a) - qbM \\ &= a'N + b'M \end{aligned}$$

This implies r is also in the set S, but r is nonnegative and strictly smaller than d. This implies $r = 0$ and $d \mid N$ and $d \mid M$.

Let $g = GCD(N, M)$. We will show that $g = d$.

Let $g = GCD(N, M)$. We will show that $g = d$.

$$\begin{aligned} d &= aN + bM \\ &= agq + bgp \\ &= g(aq + bp) \end{aligned}$$

Let $g = GCD(N, M)$. We will show that $g = d$.

$$\begin{aligned} d &= aN + bM \\ &= agq + bgp \\ &= g(aq + bp) \end{aligned}$$

This implies $g \mid d$.

Let $g = GCD(N, M)$. We will show that $g = d$.

$$\begin{aligned} d &= aN + bM \\ &= agq + bgp \\ &= g(aq + bp) \end{aligned}$$

This implies $g \mid d$. $g \leq d$.

Let $g = GCD(N, M)$. We will show that $g = d$.

$$\begin{aligned} d &= aN + bM \\ &= agq + bgp \\ &= g(aq + bp) \end{aligned}$$

This implies $g \mid d$. $g \leq d$.
Since d is smallest $d = g$

Bézout's identity
$GCD(N, M) = aN + bM$ for some $a, b \in \mathbb{Z}$.

Bézout's identity
$GCD(N, M) = aN + bM$ for some $a, b \in \mathbb{Z}$.
Exercise: Generalize this question for $N_1, N_2, N_3, \ldots, N_k$. Is it true ?

Bézout's identity

$GCD(N, M) = aN + bM$ for some $a, b \in \mathbb{Z}$.

Exercise: Generalize this question for $N_1, N_2, N_3, \ldots, N_k$. Is it true ?

This leads to an algorithm to compute GCD.

Euclid: (300 B.C.)

Input: $N \geq M \geq 0$

Euclid (N, M)

if $(M == 0)$

    then return N

    else return *Euclid* $(M, N \mod M)$

Input: X, Y

$$
\begin{array}{rl}
\text{Set} & x, y, u, v := X, Y, Y, X; \\
\text{do} & x > y \rightarrow x, v := x - y, v + u \\
\Box & y > x \rightarrow y, u := y - x, u + v \\
\text{od} & \\
\text{print} & \frac{x+y}{2}, \frac{u+v}{2}
\end{array}
$$

Fibonacci numbers:

$$0, 1, 1, 2, 3, 5, 8, 13, 22, \ldots$$

$$F(n) = F(n-1) + F(n-2), \text{ for } n \geq 2.$$

Examples:

Exercise: Number of ordered ways to partition n into parts greater than 1.

Exercise: Number of ordered ways to partition n into odd parts.

Exercise: Number of sequences of length n, consisting of 0's,1's and 2's such that 1 does not follow a 0.

Examples:

Exercise: Number of ordered ways to partition n into parts greater than 1.

Exercise: Number of ordered ways to partition n into odd parts.

Exercise: Number of sequences of length n, consisting of 0's,1's and 2's such that 1 does not follow a 0.

(X is a Fibonacci number if one of $5X^2 \pm 4$ a perfect square.)

Assertion: If $N \geq M \geq 0$ and the procedure $Euclid(N, M)$ is repeated (invoked) L times, then $N \geq F(L+2)$ and $M \geq F(L+1)$. In particular if $M \leq F(L+1)$ then the procedure is invoked at most L times.

Assertion: If $N \geq M \geq 0$ and the procedure $Euclid(N, M)$ is repeated (invoked) L times, then $N \geq F(L+2)$ and $M \geq F(L+1)$. In particular if $M \leq F(L+1)$ then the procedure is invoked at most L times.
Exercise: Use induction to prove the above statement.

Solutions for all the Fibonacci related Exercises will be provided at a later date.

Actual numerical algorithms are very "delicate" and require great care.

Actual numerical algorithms are very "delicate" and require great care.

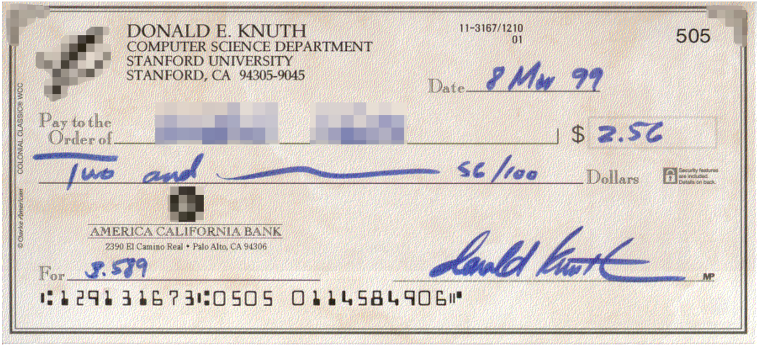
Art of Computer Programming, Volume 2: Seminumerical Algorithms by Donald Knuth

Actual numerical algorithms are very “delicate” and require great care.

Art of Computer Programming, Volume 2: Seminumerical Algorithms by Donald Knuth
Page 333 – 379 (GCD algorithm) Page 346 *Euclids Algorithm*

"I have corrected every error that alert readers detected in the second edition (as well as some mistakes that, alas, nobody noticed); and I have tried to avoid introducing new errors in the new material. However, I suppose some defects still remain, and I want to fix them as soon as possible. Therefore I will cheerfully award $2.56 to the first finder of each technical, typographical, or historical error. The webpage cited on page (iv) contains a current listing of all corrections that have been reported to me."

– *Donald Knuth*



DONALD E. KNUTH
COMPUTER SCIENCE DEPARTMENT
STANFORD UNIVERSITY
STANFORD, CA 94305-9045

11-3167/1210
01

505

Date 8 Mar 99

Pay to the Order of [redacted] $ 2.56

Two and —— 56/100 Dollars

Security features are included. Details on back.

AMERICA CALIFORNIA BANK
2390 El Camino Real • Palo Alto, CA 94306

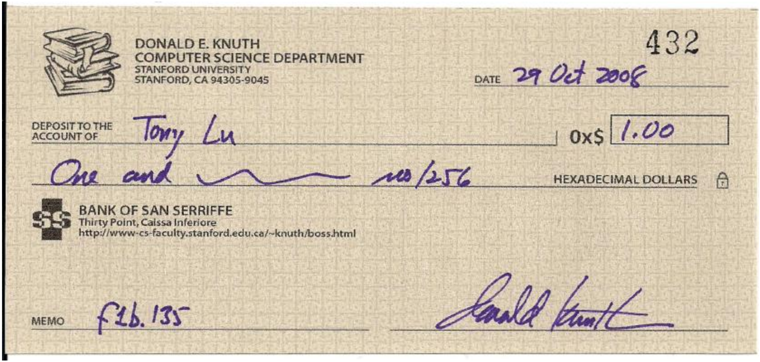
For 3.589

⑆121131673⑆0505 0114584906⑈

COLONIAL CLASSIC® WCC

© Clarke American

MP


432
DONALD E. KNUTH
COMPUTER SCIENCE DEPARTMENT
STANFORD UNIVERSITY
STANFORD, CA 94305-9045
DATE 29 Oct 2008
DEPOSIT TO THE ACCOUNT OF Tony Lu
0x$ 1.00
One and 00/256
HEXADECIMAL DOLLARS
BANK OF SAN SERRIFFE
Thirty Point, Caissa Inferiore
http://www-cs-faculty.stanford.edu.ca/~knuth/boss.html
MEMO f1b.135

Congruence - Class of residues

$$x \equiv a \mod n$$

Means n divides $x - a$.

Congruence - Class of residues

$$x \equiv a \mod n$$

Means n divides $x - a$.
The different equivalent classes can be represented by $0, 1, 2, \ldots, n-1$.

Solve:

$$x = 1 \mod 8$$

Solve:

$$x = 1 \mod 8$$

$$x = 1, 9, 17, 25, \ldots$$

Solve:

$$x = 1 \mod 8$$

$$x = 1, 9, 17, 25, \ldots$$

$x = 8k + 1$ where $k \in \{0, 1, 2, \ldots\}$

Solve:

$$x^2 = 1 \mod 8$$

Solve:

$$x^2 = 1 \mod 8$$

$$x = 1, 3, 5, 7, 9, 11, 13, 15, \ldots$$

Properties of conguences.

$$a = b \mod n \rightarrow b = a \mod n$$

Properties of conguences.

$$a = b \mod n \to b = a \mod n$$

$$a = b \mod n, b = c \mod n \Rightarrow a = c \mod n$$

Properties of conguences.

$$a = b \mod n \to b = a \mod n$$

$$a = b \mod n, b = c \mod n \Rightarrow a = c \mod n$$

$$a = a' \mod n,\ b = b' \mod n \Rightarrow a + b = a' + b' \mod n$$

Exercise:
If $a = b \mod m$ and $a = b \mod n$ then

Exercise:
If $a = b \mod m$ and $a = b \mod n$ then

$$a = b \mod (lcm(m, n))$$

Solve The following system of Equations:

$$\begin{aligned} x &= a_1 \mod n_1 \\ x &= a_2 \mod n_2 \end{aligned}$$

Given $GCD(n_1, n_2) = 1$

Case: $a_1 = a_2$

Case: $a_1 = a_2$
General case:

Case: $a_1 = a_2$
General case:
Bézouts identity‘:

$$m_1 n_1 + m_2 n_2 = 1$$

Case: $a_1 = a_2$
General case:
Bézouts identity‘:

$$m_1 n_1 + m_2 n_2 = 1$$

Set $x = a_1 m_2 n_2 + a_2 m_1 n_1$

Verification:

$$x = a_1 m_2 n_2 + a_2 m_1 n_1$$

Verification:

$$\begin{aligned} x &= a_1 m_2 n_2 + a_2 m_1 n_1 \\ &= a_1(1 - m_1 n_1) + a_2 m_1 n_1 \end{aligned}$$

Verification:

$$
\begin{aligned}
x &= a_1 m_2 n_2 + a_2 m_1 n_1 \\
&= a_1(1 - m_1 n_1) + a_2 m_1 n_1 \\
&= a_1 + (a_2 - a_1) m_1 n_1
\end{aligned}
$$

Verification:

$$\begin{aligned} x &= a_1 m_2 n_2 + a_2 m_1 n_1 \\ &= a_1(1 - m_1 n_1) + a_2 m_1 n_1 \\ &= a_1 + (a_2 - a_1) m_1 n_1 \end{aligned}$$

This implies

$$x = a_1 \mod n_1$$

What about k such equations ?

$$\begin{aligned} x &= a_1 \mod n_1 \\ x &= a_2 \mod n_2 \\ &\vdots \\ x &= a_k \mod n_k \end{aligned}$$

Where the $n_i's$ are pairwise co-prime, $(GCD(n_i, n_j) = 1)$

Let $N = \prod_{i=1}^{k} n_i$ and $N_i = \frac{N}{n_i}$.
Then we have

$$M_i N_i + m_i n_i = 1$$

Let $N = \prod_{i=1}^{k} n_i$ and $N_i = \frac{N}{n_i}$.
Then we have

$$M_i N_i + m_i n_i = 1$$

Since $GCD(N_i, n_i) = 1$

Let $N = \prod_{i=1}^{k} n_i$ and $N_i = \frac{N}{n_i}$.
Then we have

$$M_i N_i + m_i n_i = 1$$

Since $GCD(N_i, n_i) = 1$

$$x = \sum_{i=1}^{k} a_i M_i N_i$$

Let $N = \prod_{i=1}^{k} n_i$ and $N_i = \frac{N}{n_i}$.
Then we have

$$M_i N_i + m_i n_i = 1$$

Since $GCD(N_i, n_i) = 1$

$$x = \sum_{i=1}^{k} a_i M_i N_i$$

$$x = a_i M_i N_i \mod n_i = a_i(1 - m_i n_i) \mod n_i = a_i \mod n_i.$$

This is true for all $i \in \{1, 2, \ldots k\}$