Number Theory

D.M. Burton - Number Theory

- **Well-Ordering Principle**: Every non-empty set S of non-negative integers contains a least element.

  Example: $n < 2^n \ \forall\ n \in \mathbb{Z}^+$

- **Theorem** (Archimedean Property): If a and b are any positive integers, then there exists a positive integer n s.t. $na \geq b$.

  proof: (by contradiction).

  Let the property does not hold.

  i.e. $\exists$ some a, b for which $na < b$ $\forall$ positive integer n.

  Then $S = \{ b - na \mid n \text{ is a positive integer} \}$ is a non-empty set of non-negative integers.

  $\therefore$ By well-ordering principle, S must have a least element, say $b - ma$, m is a positive integer.

  Note that $b - (m+1)a \in S$ and $b - (m+1)a < b - ma$

  as $ma < b \Rightarrow (m+1)a = ma + a < b + a < b$ ($\rightarrow\leftarrow$)

  Hence Statement of the theorem must be true.

- **Theorem** (First Principle of finite Induction): Let S be a set of positive integers with the following properties:

  (a) The integer $1 \in S$ (Basis for the induction)

  (b) Whenever the integer $k \in S$, the next integer $k+1$ must also $\in S$. (Induction Step).

  Then S is the set of all positive integers.

  prove that $0 < a - 1 < a$

  - a least elmt of T $\Rightarrow \boxed{a-1 < a}$
  - $1 \in S \Rightarrow a \neq 1$ (a ∈ T)
  - 1 least elmt of $\mathbb{N}$ $\Rightarrow a \neq 1$
  - $\Rightarrow a > 1$
  - $\Rightarrow \boxed{a-1 > 0}$

  proof: Let $T \neq \emptyset$ be the set of all positive integers not in S.

  Then by Well-Ordering Principle, T must have a least element, say a.

  ~~Now $a \in T$ & $1 \in$~~

  [$S \cup T$ = the set of all positive integers.]

  Then $0 < a-1 < a \Rightarrow a-1 \notin T$ (a least elmt of T) $\Rightarrow a-1 \in S$ $\Rightarrow a \in S$ (as S is closed by (b))

As $1 \in S$, we have $a > 1 \Rightarrow 0 < a-1 < a \Rightarrow a-1 \notin T$ as a is the smallest element of T

$\Rightarrow a-1 \in S$.

Then by hypothesis, S must contain $(a-1)+1 = a$ $(\rightarrow\leftarrow)$ as $a \in T$ & $S \cap T = \emptyset$.

Hence our initial assumption that $T \neq \emptyset$ is wrong

$\Rightarrow T = \emptyset$ i.e. S contains all the positive integers.

Theorem: (Second Principle of Finite Induction): Let S be a set of positive integers with the following properties

(a) The integer $1 \in S$ (Basis)

(b) If k is a positive integer s.t. $1, 2, \cdots, k \in S$, then $k+1$ must also be in S. (Induction hypothesis).

Then $S = N$

proof Let T be the set of all positive integers not in S. $T = N \setminus S$

Claim $T = \emptyset$

Let us assume that $T \neq \emptyset$.

Then be the Well-Ordering Principle, T must have a least element, say, n.

As $1 \in S$, we have $n > 1 \Rightarrow 0 < n-1 < n$

Minimal nature of $n \in T \Rightarrow$ none of $1, 2, \cdots, n-1$ $\Rightarrow 1, 2, \cdots, n-1 \in S$.

$\Rightarrow (n-1)+1 = n \in S$ by induction hypothesis $(\rightarrow\leftarrow)$ to the choice of n

Hence $T = \emptyset$ i.e. S contains all the positive integers.

Example: (first Principle of finite Induction)

Mention only $1+2+2^2+\cdots+2^{k-1} = 2^k - 1$ ——— (1)

Soln. Let S be the set of all positive integers k for which equn (1) holds.

Base $k=1$ (1) holds

Induction Let (1) holds for n i.e. $n \in S$

i.e. $1+2+2^2+\cdots+2^{n-1} = 2^n - 1$.

$\Rightarrow 1+2+2^2+\cdots+2^{n-1}+2^n = (2^n-1)+2^n = 2\cdot 2^n - 1 = 2^{n+1}-1$

$\Rightarrow$ (1) holds for $n+1$. $\Rightarrow n+1 \in S$.

Hence by induction principle, S is the set of all positive integers.

In other words, equn (1) holds $\forall$ +ve integers k.

Disadvantage of induction

- No aid in formulating such statements.
- "educated guess" is made at a property that is believed might hold in general.
- for instance,

$1 = 1 = 2-1$
$1+2 = 3 = 2^2-1$
$1+2+2^2 = 7 = 2^3-1$
$1+2+2^2+2^3 = 15 = 2^4-1$

Guess for a rule $\rightarrow$ $1+2+2^2+\cdots+2^n = 2^{n+1}-1$.

Example (educated guess may not work).

$p(n) \to$ # of partitions of n

i.e. # of different ways to write n as a sum of +ve integers, disregarding order.

e.g. $p(1) = 1$

$p(2) = 2$

$p(3) = 3$

$p(4) = 5$

$p(5) = 7$

↓

runs through prime numbers.

$p(6) = 11$

1 → 1

2 → 1+1, 2

3 → 1+2, 2+1, 3

1 → 1

2 → 2, 1+1

3 → 3, 2+1, 1+1+1

4 → 4, 3+1, 2+2, 2+1+1, 1+1+1+1

5 → 5, 4+1, 3+2, 3+1+1, 1+1+1+2, 2+1+2, 1+1+1+1+1

Conjecture $p(n)$ is prime.

Unfortunately, $p(7) = 15$, spoiling everything.

- $p(n)$ are known to be quite complicated.

(G.H. Hardy, Ramanujan (London: Cambridge University Press, 1940) chapter 8, p. 6, 8.)

Example: (Second Principle of finite Induction).

Lucas sequence:

1, 3, 4, 7, 11, 18, 29, 47, 76, ...

Except the first two terms, each term of this sequence is the sum of the preceding two.

The sequence may be defined inductively by

$$a_1 = 1$$
$$a_2 = 3$$
$$a_n = a_{n-1} + a_{n-2} \quad \text{for all } n \geq 3.$$

Claim $\boxed{a_n < \left(\frac{7}{4}\right)^n}$ $\forall$ positive integer n.

Base: $a_1 = 1 < \frac{7}{4}$

$a_2 = 3 < \frac{16}{16} < \left(\frac{7}{4}\right)^2$

Induction: Assume that the inequality is valid for $n = 1, 2, \cdots, k-1$ when $k \geq 3$, a positive integer.

Then, in particular, $a_{k-1} < \left(\frac{7}{4}\right)^{k-1}$, $a_{k-2} < \left(\frac{7}{4}\right)^{k-2}$

Now $a_k = a_{k-1} + a_{k-2}$

$$< \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^{k-2}$$
$$= \left(\frac{7}{4}\right)^{k-2}\left[\frac{7}{4} + 1\right]$$
$$= \left(\frac{7}{4}\right)^{k-2}\left(\frac{11}{4}\right).$$
$$< \left(\frac{7}{4}\right)^{k-2}\left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^k$$

$\frac{11}{4} < \frac{7}{4}$ $\cdot$ $\frac{7}{4}$

$\frac{44}{16} = \frac{11 \times 4}{4 \times 4} < \frac{49}{16}$

Thus the inequality holds for k whenever it holds for the integers $1, 2, \cdots, k-1$.

Also it holds for $n = 1, 2$

$\therefore$ By the second induction principle $a_n < \left(\frac{7}{4}\right)^n$ $\forall$ $n \geq 1$

Tom M. Apostol - Introduction to Analytic Number Theory.

Division Algorithm

If a and b are integers with $b \geq 1$, then there exists unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < b$$

(q is called the quotient and r is called remainder in the division of a by b.)

proof.

Let us consider the subset of integers

$$S = \{ a - bx \mid x \in \mathbb{Z},\ a - bx \geq 0 \}$$

Claim 1: S is non-empty

proof: Since $b \geq 1$, $|a|b \geq |a|$

$$\therefore a + |a|b \geq a + |a| \geq 0$$

or $a - xb \geq 0$ for $x = -|a|$.

$\Rightarrow$ S is non-empty.

Since S is a non-empty set of non-negative integers, either

(i) S contains 0 as its least element or

(ii) S contains a smallest positive integer as its least element

(by the well-ordering principle of the set of all natural numbers $N = \{1, 2, 3, \cdots\}$)

The well-ordering principle: If A is a non-empty set of positive integers, then A contains a least element

In either case, we call it r.

Therefore, there exists an integer q such that

$$a - bq = r, \quad r \geq 0.$$

Claim 2:
We assert that $r < b$.

proof: If not, $r \geq b$ & therefore

$$a - (q+1)b = (a - qb) - b = r - b \geq 0$$

This shows that $a - (q+1)b \in S$ and also $a - (q+1)b = r - b < r$, which leads to a contradiction to the fact that r is the least element in S.

Hence $r < b$.

Claim 3: ~~Uniqueness of~~ Integers q and r are unique.

proof:
In order to establish uniqueness of q and r, let us suppose that a has two representations.

$a = bq + r$, $a = bq' + r'$, where $0 \leq r < b$, $0 \leq r' < b$.

Then $b(q - q') = r' - r$

or $b|q - q'| = |r' - r|$

But $0 \leq r' < b$ and $-b < -r \leq 0 \Rightarrow -b < r' - r < b$
i.e. $|r' - r| < b$.

$\therefore |q - q'| < 1$

Since q & q' are integers, the only possibility is

$q = q'$.

Therefore, $r = r'$ and the proof is complete.

Theorem: Given integers a and b, with $b \neq 0$, $\exists$ unique integers q and r such that $a = bq + r$, $0 \leq r < |b|$

proof:
~~Case $b > 0$~~ Case $b \geq 1$: follows by Division algm.

Case $b < 0$: $|b| > 0$ $\therefore a = |b|q' + r$, $0 \leq r < |b|$
$= -bq' + r$, $q' = -q$
$= bq + r$

(3) (5)

Theorem: Suppose that a and b are integers not both equal to zero, and let $d = \gcd(a, b)$. Then there exist integers x and y such that $d = ax + by$. In the special case in which a and b are relatively prime, we can write $1 = ax + by$.

↳ existential proof ↳ gives no means to calculate gcd(a,b), a, b

proof: Let $S = \{ax + by \mid x, y \in \mathbb{Z} \text{ and } ax + by \text{ is positive}\}$.

same as in FTA

Claim: S is a non-empty set.

proof: Since at least one of a, b is non zero, let $a \neq 0$. Then $|a| > 0$.

$\therefore |a| = a \cdot x + b \cdot 0$ is an element of S, where we choose $x = \begin{cases} 1 & \text{if } a > 0 \\ -1 & \text{if } a < 0. \end{cases}$

Since S is non-empty set of positive integers, by the well ordering principle, S contains a least element, say, d.

$\therefore d = au + bv$ for some integers u, v.

Claim: d is a common divisor of a & b.

Now by division algorithm, $a = dq + r$ where q, r are integers and $0 \leq r < d$.

$\therefore r = a - dq$
$= a - (au + bv)q$
$= a(1 - uq) + b(-vq)$

This representation shows that $r \in S$. Also $r < d$ (⋆)

But $0 \leq r < d$ and since d is the least element in S, $r = 0$.

if $r \neq 0$

This proves that $a = dq$ which means d is a divisor of a. By similar arguments, we can prove that d is a divisor of b.

Therefore, d is a common divisor of a and b.

Claim: d is the $\gcd(a,b)$.

To prove that d is the $\gcd(a,b)$, let us assume that c is a common divisor of a and b.

Then $c \mid a$ and $c \mid b$.

$\therefore c \mid au + bv$ (by linearity property of divisibility).

i.e. $c \mid d$ and this proves d is the greatest common divisor.

The Euclidean Algorithm

The Euclidean algm. consists of repeatedly applying the division algm. It is based on the following simple property:

Fact: If a, b, q and r are as in the division algm; then $[a = bq + r,\ 0 \le r < b]$

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

proof. From the equation $a = bq + r$ — (1).

If $e \mid r$ and $e \mid b$, then $e \mid a$.

Rewriting equⁿ. (1)

$$r = a - bq.$$

If $e \mid a$ and $e \mid b$, then $e \mid r$

We have proved that the set of all common divisors of r and b equals the set of all common divisors of a and b, from which the result of the theorem directly follows.

Algorithm : The Euclidean Algorithm.

Input : A pair of integers a and b, not both equal to 0.

Output : The greatest common divisor, $\gcd(a,b)$.

We may assume that $a \geq b$ (if not switch a and b).

Apply the division algorithm to write

$$a = q_0 b + r_1 .$$

If $r_1 = 0$, then $\gcd(a,b) = b$

Otherwise, continue by dividing successive divisors by successive remainders until a zero remainder is reached :

$$b = q_1 r_1 + r_2 , \quad 0 \leq r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 , \quad 0 \leq r_3 < r_2$$

$$\cdots$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n , \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = q_n r_n + 0$$

The last non-zero remainder r_n is $\gcd(a,b)$.

Since the sequence of successive remainders is strictly decreasing, $b > r_1 > r_2 > \cdots > r_n > 0$, the algm. must eventually terminate (at most b steps).

Since $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \gcd(r_2,r_3)$

$= \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n$,

it follows that $\gcd(a,b) = r_n$, the last non-zero remainder that is encountered in this process.

Input : two non-negative integers a and b with $a \geq b$

Output : the $\gcd(a,b)$.

$b \mid a \mid q$

$r \mid b \mid$

1. While $(b \neq 0)$ do the following

   set $r \leftarrow a \bmod b$;

   $a \leftarrow b$;

   $b \leftarrow r$;

2. Return (a);

loop at most b times, b constant.

Time complexity : $O\left((\ln(n))^2\right)$ bit operations.

- $a,b \in \mathbb{N}$, $a,b \leq n$

  # of bits in binary representation of $n \rightarrow \lfloor \log n \rfloor + 1$

operations		bit complexity
Addition :	$a+b$	$\rightarrow O(\log a + \log b) = O(\log n)$.
Subtraction :	$a-b$	$\rightarrow O(\log a + \log b) = O(\log n)$
Multiplication :	$a \cdot b$	$\rightarrow O((\log a)(\log b)) = O((\log n)^2)$
Division :	$a = bq + r$	$\rightarrow O((\log q)(\log b)) = O((\log n)^2)$

Theorem (fundamental Theorem of Arithmetic):

Every positive integer $a > 1$ can be uniquely expressed as the product of primes.

(In other words, there exist unique prime numbers $p_1 < p_2 < \cdots < p_n$ and corresponding positive exponents $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}_+$ such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}.$$

[Note: This important theorem is the reason why the number 1 is not considered to be prime. If 1 were prime, we would no longer have unique factorization; for example, $18 = 2 \cdot 3^2 = 1^3 \cdot 2 \cdot 3^2 = 1^{12} \cdot 2 \cdot 3^2$, and so forth.]

proof:

Part I: (Existence)

Suppose that there were positive integers greater than 1 that were not expressible as a product of primes.

Let n be smallest such integer.

Since n cannot be prime (because a single prime is a product of primes), it must be composite.

So we can write $n = ab$, where a and b are smaller integers with $1 < a, b < n$.

But since n was chosen to be the smallest integer that cannot be written as a product of primes, both a and b must be expressible as a product of primes.

Since $n = ab$, we can multiply prime factorizations of a and b to obtain a prime factorization of n. With this contradiction, the existence proof is complete.

Part II : (Uniqueness)

Suppose that a positive integer n had two different prime factorizations :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$$

where $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_l$ are primes, and $\alpha_1, \alpha_2, \cdots, \alpha_k$ and $\beta_1, \beta_2, \cdots, \beta_l$ are positive exponents.

If there are any primes among the p's and q's that are common, they can be divided through (cancelled) on both sides of the equation so that the lists $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_l$ can be assumed to have no primes in common, and we assume that this is indeed the case. i.e. no common primes among p's and q's. in the lists $p_1 < p_2 < \cdots < p_k$ & $q_1 < q_2 < \cdots < q_l$.

Now since $p_1 \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$, it follows by Euclid's lemma that $p_1 \mid q_j$ for some index j.

But since p_1 and q_j are both primes, it follows that $p_1 = q_j$, which contradicts the assumption that the p's & q's have no primes in common. This completes the Uniqueness proof.

Alternative proof (using Strong induction)

Base:

$P(n)$: n has prime factorization

$P(2)$ true as 2 is product of 1 prime (itself)

Inductive step:

WT $P(2), \ldots P(k)$ all true.

Consider $P(k+1)$ → $k+1$ prime done.

→ $k+1$ composite

So $k+1 = ab$, $1 \leq a, b \leq k$

So $P(a), P(b)$ true by induction hypothesis.

So $P(k+1)$ true.

↳ consists of prime factorization of a as well as b.

Def^n The integers modulo n, $\mathbb{Z}_n$, is the set of integers

$$\{0, 1, 2, \cdots, n-1\}.$$

Addition, subtraction, and multiplication in $\mathbb{Z}_n$ are performed modulo n.

Def^n Let $a \in \mathbb{Z}_n$. The multiplicative inverse of a modulo n is an integer $x \in \mathbb{Z}_n$ s.t. $ax \equiv 1 \pmod{n}$.

If such an x exists, it is unique, and a is said to be invertible or a unit; the inverse of a is denoted by $\bar{a}^1$.

Def^n Let $a, b \in \mathbb{Z}_n$. Division of a by b modulo n is the product of a and b^{-1} modulo n, and is only defined if b is invertible modulo n.

(proof) **Fact** Let $a \in \mathbb{Z}_n$. Then a is invertible iff $\gcd(a, n) = 1$.

(proof) **Fact** Let $d = \gcd(a, n)$. The congruence equation

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

has a solution x iff d divides b, in which case there are exactly d solutions between 0 and $n-1$; these solutions are all congruent modulo n/d.

Exercises: Find all solutions of the following congruences

(a) $123x \equiv 13 \pmod{456}$

(b) $15x + 4 \equiv 20 \pmod{25}$.

Algorithm: (Procedure for solving $ax \equiv c \pmod m$ in the case $d = \gcd(a,m) > 1$ and $d \mid c$).

Recall that if $d \nmid c$, there are no sol^{n}s.

Step-1: Solve the modified congruence

$$\frac{a}{d} y \equiv \left(\frac{c}{d}\right) \bmod \left(\frac{m}{d}\right)$$

This is possible, and there will be a unique sol^n: y_0, since $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$.

Step-2: The d solutions of the original congruence are $y_0, y_0 + \frac{m}{d}, y_0 + \frac{2m}{d}, \ldots, y_0 + \frac{(d-1)m}{d}$ $\pmod m$

Example: find all sol^{n}s of the following congruences:

(a) $2x \equiv 7 \pmod{10}$ $\quad \gcd(2,10) = 2 \nmid 7$

$\rightarrow$ no sol^n.

(b) $6x \equiv 12 \pmod{21}$ $\quad \gcd(6,21) = 3 \mid 12$

so 3 sol^{n}s.

$2y \equiv 4 \pmod 7$ has unique sol^n.

$y_0 = 2^{-1} \times 4 \pmod 7$ $\quad 2^{-1} \bmod 7 = 4$

$= 16 \pmod 7$ $\quad 4 \cdot 2 = 8 = 1 \bmod 7$.

$\equiv 2 \pmod 7$. $\quad \{2, 2+\frac{21}{3}, 2+2\cdot\frac{21}{3}\} = \{2, 9, 16\}$.

$\gcd(2,7) = 1 = 2u + 7v$

$1 \equiv 2u \bmod 7$

find u, v by Extended Euclid's algo.

(Proof) **Fact** (Chinese remainder theorem, CRT)

If the integers $n_1, n_2, \ldots, n_k$ are pairwise relatively prime, then the system of simultaneous congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

has a unique solution modulo $n = n_1 n_2 \cdots n_k$.

Algorithm (Gauss's algorithm)

The solution x to the simultaneous congruences in the Chinese remainder theorem may be computed as

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

where $N_i = n/n_i$ and $M_i = N_i^{-1} \mod n_i$.

Time complexity $O\left((\log n)^2\right)$ bit operations.

Example: $\left.\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 7 \pmod{13} \end{aligned}\right\}$ has a unique soln. $x \equiv 59 \pmod{91}$.

Fact If $\gcd(n_1, n_2) = 1$, then the pair of congruences

$$x \equiv a \pmod{n_1}$$
$$x \equiv a \pmod{n_2}$$

has a unique solution

$$x \equiv a \pmod{n_1 n_2}.$$

$$x = 3 \times 13 \times (13^{-1} \bmod 7) + 7 \times 7 \times (7^{-1} \bmod 13)$$
$$= 3 \times 13 \times 6 + 7 \times 7 \times 2 \pmod{91}$$
$$= 332$$
$$\equiv 59 \pmod{91}$$

Example:

Solve the following system of congruences:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 6 \pmod{14}$$

$n_1 = 3$, $n_2 = 5$, $n_3 = 14$

pairwise relatively prime

↓

sol^n exists.

Sol^n:

$n = n_1 \times n_2 \times n_3 = 210$.

$a_1 = 2, a_2 = 3, a_3 = 6$.

$N_1 = \frac{210}{3} = 70$, $N_2 = \frac{210}{5} = 42$, $N_3 = \frac{210}{14} = 15$.

$M_1 = 70^{-1} \bmod 3 = 1$

$M_2 = 42^{-1} \bmod 5 = 3$

$M_3 = 15^{-1} \bmod 14 = 1$

$70 \times 1 \bmod 3 = 1 \bmod 3$

$42 \times 3 \bmod 5 = 126 \bmod 5 = 1 \bmod 5$

$15 \times 1 \bmod 14 = 1 \bmod 14$

$x \equiv 2 \times 70 \times 1 + 3 \times 42 \times 3 + 6 \times 15 \times 1 \bmod 210$

$\equiv 608 \bmod 210$

$= 188$.

Def^n: The multiplicative group of $\mathbb{Z}_n$ is

$$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \mid \gcd(a,n) = 1 \}.$$

In particular, if n is a prime, then

$$\mathbb{Z}_n^* = \{ a \mid 1 \le a \le n-1 \}.$$

$$= \{ 1, 2, \cdots, n-1 \}.$$

Def^n: The order of $\mathbb{Z}_n^*$ is defined to be the number of elements in $\mathbb{Z}_n^*$, namely $|\mathbb{Z}_n^*|$.

Note. It follows from the definition of the Euler phi function that $|\mathbb{Z}_n^*| = \phi(n)$.

Note. $\mathbb{Z}_n^*$ is closed under multiplication ($a \in \mathbb{Z}_n^* \And b \in \mathbb{Z}_n^* \Rightarrow a \cdot b \in \mathbb{Z}_n^*$).

Fact Let $n \ge 2$ be an integer.

(i) (Euler's theorem) If $a \in \mathbb{Z}_n^*$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

(ii) If n is a product of distinct primes, and if $r \equiv s \pmod{\phi(n)}$, then

$$a^r \equiv a^s \pmod{n}$$

for all integers a.

proof $r - s = q\phi(n)$, $q \in \mathbb{Z}$

$r = s + q\phi(n)$

$a^r = a^s \cdot (a^{\phi(n)})^q \equiv a^s \cdot 1^q = a^s \pmod{n}$

In other words, when working modulo such an n, exponents can be reduced modulo $\phi(n)$.

A special case of Euler's theorem is Fermat's (little) theorem.

Fact Let p be a prime.

(proof) (i) (Fermat's theorem) If $\gcd(a,p)=1$, then $a^{p-1} \equiv 1 \pmod{p}$

(ii) If $r \equiv s \pmod{p-1}$, then $a^r \equiv a^s \pmod{p}$ for all integers a.

In otherwords, when working modulo a prime p, exponents can be reduced modulo $p-1$.

(iii) In particular, $a^p \equiv a \pmod{p}$ for all integers a.

Defn Let $a \in Z_n^*$. The order of a, denoted by $\text{ord}(a)$, is the least positive integer t such that $a^t \equiv 1 \pmod{n}$.

(proof)

Fact If the order of $a \in Z_n^*$ is t, and $a^s \equiv 1 \pmod{n}$, then t divides s. In particular, $t \mid \phi(n)$.

Example Let $n=21$

Then $Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

Note that $\phi(21) = \phi(3)\phi(7)$
$= 2 \times 6 = 12. = |Z_{21}^*|$

The orders of elements in Z_{21}^*

$a \in Z_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
order of a	1	6	3	6	2	6	6	2	3	6	6	2

(Check)

Defn Let $\alpha \in Z_n^*$. If the order of α is $\phi(n)$, then α is said to be a generator or a primitive element of Z_n^*.

If Z_n^* has a generator, then Z_n^* is said to be cyclic.

$\alpha \to$ primitive root mod n

Fact (properties of generators of Z_n^*) (Existence and Number of primitive roots)

(i) Z_n^* has a generator iff $n = 2, 4, p^k$ or $2p^k$, where p is an odd prime and $k \geq 1$. In particular, if p is prime, then Z_p^* has a generator. (Existence of primitive roots)

(ii) If α is a generator of Z_n^*, then $Z_n^* = \{\alpha^i \bmod n \mid 0 \leq i \leq \phi(n)-1\}$.

(iii) Suppose that α is a generator of Z_n^*. Then $b = \alpha^i \bmod n$ is also a generator of Z_n^* iff $\gcd(i, \phi(n)) = 1$. (# of primitive roots)

$\left[Z_{\phi(n)}^* = \{i \in Z_{\phi(n)} \mid \gcd(i, \phi(n)) = 1\}\right.$

$\left.|Z_{\phi(n)}^*| = \phi(\phi(n))\right]$

It follows that if Z_n^* is cyclic, then the number of generators is $\phi(\phi(n))$.

(iv) $\alpha \in Z_n^*$ is a generator of Z_n^* iff $\alpha^{\phi(n)/p} \not\equiv 1 \pmod n$ for each prime divisor p of $\phi(n)$.

Example: Z_{21}^* is not cyclic since it does not contain an element of order $\phi(21) = 12$.

Note that 21 is not of the form p^k or $2p^k$, where p is an odd prime & $k \geq 1$.

$\phi(25) = \phi(5)\phi(5) = 4 \times 4 = 16$

$2^{\phi(25)} = 2^{16} = 2^{10} \cdot 2^6 \equiv 24 \times 7 \times 2 \pmod{25} \equiv 168 \times 2 \pmod{25}$

Example: Z_{25}^* is cyclic, & has a generator $\alpha = 2$.

$|Z_{25}^*| = \phi(25) = \phi(5^2) = 25(1-\frac{1}{5}) = 25(\frac{4}{5}) = 20$

$a \in Z_{25}^*$	1	2	3	4	6	7	8	9	11	12	13	14	16	17	18	19	21	22	23	24
order of a	1	20																		

# of generators in Z_{25}^* is $\phi(\phi(25)) = \phi(20) = 8$.
If the generator is $\alpha = 2$. $= 20(1-\frac{1}{5})(1-\frac{1}{2})$

Z_{25}^*

check $2^{20} \equiv 1$

$\alpha = 2$ is a generator. → order of $\alpha = 20$

$\phi(25) = 20$,

Z_{20}^*

$\phi(\phi(25)) = \phi(20) = 8$ → many generators.

$$Z_{\phi(25)}^* = \{ i \in Z_{\phi(n)} \mid \gcd(i, \phi(n)) = 1 \}$$

$$Z_{20}^* = \{ i \in Z_{20} \mid \gcd(i, 20) = 1 \}$$

$$= \{1, 3, 7, 9, 11, 13, 17, 19\}$$

$|Z_{20}^*| = 8 = \phi(\phi(25))$.

$$\boxed{\alpha^i \bmod 25 \;,\; i \in Z_{20}^*}$$

↓ all generators

$\{2, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}, 2^{19} \bmod 25\}$

$= \{2, 8, 3, 12, 23, 17, 22, 13\}$.

$2^{13} = 2^{10} \cdot 2^3 = 1024 \times 8 \bmod 25 = 24 \cdot 7 \times 4$

$2^5 = 32$
$= 7 \times 4$
$= 28$
$= 3.$

$2^9 = 3 \times 4$
$= 12$

$2^{11} = 12 \times 4$
$= 48$
25
$\overline{23}$

$2^{13} = 23 \times 4$
$= 92$
75
$\overline{17}$

$2^{17} = 2^{13} \times 2^4$
$= 17 \times 16$
$= 34 \times 8$
$= 9 \times 8$
$= 72$
50
$\overline{22}$

17×8
$25 \mid 136 \mid 5$
125
$\overline{11}$ 26

$2^{19} = 22 \times 4$
$= 88$
75
$\overline{13}$

$2^{19} = 7 \times 4$
$= 28$
25
$\overline{3}$

$\text{ord}_{25}(7) = 4 \mid \phi(25) = 20.$

$7^4 \bmod 25$
$= 49 \times 49 \bmod 25$
$= 24 \times 24 \bmod 25$
$= 36 \times 16 \bmod 25$
$= 11 \times 16 \bmod 25$
$= 44 \times 4 \bmod 25$
$= 19 \times 4 \bmod 25$
$= 38 \times 2 \bmod 25$
$= 13 \times 2 \bmod 25$
$= 1 \bmod 25.$

$\mathbb{Z}_{13}^* = \langle 6 \rangle.$

Exercise → Find all the generators of $\mathbb{Z}_{13}^*$.

Soln. $p = 13$. $\phi(13) = 12$. $\therefore$ order of $\alpha = 6$ is 12.

$\alpha = 6$

$|\mathbb{Z}_{12}^*| = \phi(\phi(13)) = \phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4.$

$\mathbb{Z}_{12}^* = \{ i \in \mathbb{Z}_{12} \mid \gcd(i, 12) = 1 \} = \{1, 5, 7, 11\}.$

cyclic gp.

$|\mathbb{Z}_{13}^*| = 12.$
$= \phi(13).$

generators of $\mathbb{Z}_{13}^*$

$\{6^1, 6^5, 6^7, 6^{11} \text{ modulo } 13\}$
$= \{6, 12, 3, 10\}.$

check $6^{12} \equiv 1 \pmod{13}$.
$12^{12}, 3^{12}, 10^{12} \equiv 1 \pmod{13}$

Example: for which of the following moduli n do primitive roots exist?

In cases where primitive roots exist, how many will there be (mod n)?

(a) $n = 20$, (b) $n = 59$, (c) $n = 30$, (d) $n = 1250$.

$20 = 2^2 \cdot 5$

$59 =$

$30 = 2 \cdot 3 \cdot 5$

$1250 = 2 \cdot 5^4$.

have primitive roots.

How many primitive roots

$\phi(\phi(59)) = \phi(58)$

$= \phi(2 \cdot 29) = 28$.

primitive roots (mod 59)

$\phi(\phi(1250)) = \phi(\phi(2 \cdot 5^4))$

$= \phi(500) = \phi(2^2 \cdot 5^3)$

$= 200$

primitive roots (mod 1250)

Some Natural Questions

1. Existence of primitive roots → for which moduli n?
2. Finding Primitive Roots → Deterministic
3. Computing orders → Find $\text{ord}_n(a)$? $\gcd(a, n) = 1$
4. The Discrete Logarithm Problem (DLP) → g is primitive root mod n

$\forall\ a \in \mathbb{Z}, \gcd(a, n) = 1$

find j s.t. $g^j \equiv a \pmod n$

unique mod $\phi(n)$

DLP

Determination of Primitive Roots

finding primitive roots (when they exist)

convert ⟹ Determination of primitive roots modulo a prime

Theorem modulus n, primitive roots mod n exists if $n = 2, 4, p^k$ or $2p^k$, p some odd prime, $k \in \mathbb{Z}^+$

In each of the cases for a modulus n in which primitive roots exist, the following rules show how primitive roots can be found:

Algm. (b) → (c) → (a)

(a) If g is a primitive root modulo an odd prime power p^k, then g or $g+p^k$ (whichever is odd) will be a primitive root mod $2p^k$.

(b) If g is a primitive root modulo an odd prime p, then g or $g+p$ (whichever is odd) will be a primitive root mod p^2.

Z_5^* 2,3 → $Z_{5^2}^*$ 2,3

(c) If p is an odd prime and g is a primitive root mod p^2, then g will also be a primitive root mod any higher power p^k of p.

$Z_{2\times5^2}^*$ 7,3

$\phi(\phi(7)) = \phi(7-1) = \phi(6) = \phi(3)\phi(2) = (3-1)(2-1) = 2 \times 1 = 2$

Example. (1) no primitive roots modulo 8.

(2) primitive roots modulo $7 \to 3, 5$.

⟹ 3 is a primitive root mod 7^2

Also 5 is a primitive root mod 7^2

⟹ 3 is a primitive root mod 7^k, $k > 2$, $k \in \mathbb{Z}^+$

Also 5 . . . . .

⟹ 3 is a primitive root mod 2×7^k, $k > 2$, $k \in \mathbb{Z}^+$

Also 5 . . . . . .

Week 8

Euclidean Algorithm

Input : two non-negative integers a and b with $a \geq b$

Output : gcd(a,b)

1. $x = a$; $y = b$
2. if $y = 0$ return $x = gcd(a,b)$
3. $r = x \bmod y$
4. $x \leftarrow y$
5. $y \leftarrow r$
6. goto 2

$y \mid x$

$r \mid y$

At each iteration

- x is replaced by previous value of y
- y is replaced by $x \bmod y$

Time complexity : $O((\log n)^2)$ bit operations

The Extended Euclidean Algorithm

Input: A pair of positive integers a and b, with $a \geq b$.

Output: Three integers, $d = \gcd(a,b)$, x, and y, that satisfy the equation $d = ax + by$. (x, y not necessarily unique)

Step 1. Set $U = [a, 1, 0]$, $V = [b, 0, 1]$
(initialize recordkeeping vectors)

Step 2. While $(V(1) > 0)$
(Tasks below will be repeated whilst first component of V is positive)

$$W = V - \left\lfloor \frac{U(1)}{V(1)} \right\rfloor V$$

$V \mid U \mid Q = \frac{V[1]}{V[1]}$
$W \mid V \mid$

Update: $U = V$

Update: $V = W$

end (while)

Step 3. (Output: $d = V(1)$, $x = U(2)$, $y = U(3)$.

$Q = \frac{V(1)}{V(1)}$

$a = 1769, b = 550$

Q	U_1	U_2	U_3	V_1	V_2	V_3
–	1769	1	0	550	0	1
3	550	0	1	119	1	-3

(3)

Example: (a) Compute $d = \gcd(148, 75)$ and integers x and y such that $d = 148x + 75y$ (Ans. $d=1$, $x=37$, $y=-73$)

(b) If it exists, compute the $75^{-1} \bmod 148$. (Ans. 75 or -73)

Example: (a) Compute $d = \gcd(4864, 3458)$ (Ans. $d=38$)
$a \quad b$

~~(b) $d = ax + by$~~ for integers x and y such that

$d = 4864x + 3458y$ (Ans. $x = 32, y = -45$)

Lame's Theorem: # of divisions $\leq 5(\log_{10} b + 1)$

- Time complexity $O((\log n)^2)$ bit operations

$d = 1769(-171) + 550(550)$
$= 1769(-171 + 550) + 550(550 - 1769)$
$= 1769(379) + 550(-1219)$.
$x \quad y$

- Extended Euclidean Algm. is just the Euclidean algm, with some additional recordkeeping.
- Compute $d = \gcd(1769, 550)$ & integers x and y s.t.

$d = 1769x + 550y$.

$V_1 = U_1 - QV_1 = 1769 - 3 \times 550$
$V_2 = U_2 - QV_2 = 1 - 3 \times 0$
$V_3 = V_3 - QV_3 = 0 - 3 \times 1$

$d = 3$ ~~$d = 1$~~
~~$x = 37$~~ $x = -171$
$y = -119$ $y = 550$

$V_1 = U_1, V_2 = U_2, V_3 = V_3$

$\frac{U_1}{V_1} = Q$	U_1	U_2	U_3	V_1	V_2	V_3
—	1769	1	0	550	0	1
3	550	0	1	119	1	-3
4	119	1	-3	74	-4	13
1	74	-4	13	45	5	-16
1	45	5	-16	29	-9	29
1	29	-9	29	16	14	-45
1	16	14	-45	13	-23	74
1	13	-23	74	3	37	-119
4	3	37	-119	1	-171	550
3	1	-171	550	0	—	—

$V_1 = 550 - 4 \times 119 = 550 - 476 = 74$
$V_2 = 0 - 4 \times 1 = -4$
$V_3 = 1 - 4 \times (-3) = 13$

$3 - 3.1$
~~37~~ $3.(-171)$
~~580~~ $-3(550)$
$-119 \quad 1 - 3.1$
~~-171~~
$-171 - 3.$

Example: a) Compute $d = \gcd(148, 75)$ and integers x, y s.t. $d = 148x + 75y$. (4)

(b) If it exists, compute $75^{-1} \bmod 148$.

Sol^n:

$Q = \frac{V[1]}{V[1]}$	$U[1]$	$U[2]$	$U[3]$	$V[1]$	$V[2]$	$V[3]$
–	148	1	0	75	0	1
1	75	0	1	73	1	-1
1	73	1	-1	2	-1	2
36	2	-1	2	1	37	-73
2	1 ↓ $\gcd(148, 75)$	37 ↓ x	-73 ↓ y	0	-75	-144

$2 - 146$

~~$1 = 37 \times 148 - 37 \times 75$~~

~~$= 37 \times 148 + 75 \times (-3$~~

$d = 1$

$x = 37$

$y = -73$.

$1 = 37 \times 148 + (-73) \times 75$

$1 \equiv (-73) \times 75 \pmod{148}$

$\Rightarrow 75^{-1} \bmod 148 = -73.$

$= 148 - 73$

$= 75$

~~x, y~~ not unique

$1 = d = 148(37) + 75(-73)$

$= 148(37 + 75) + 75(-73 - 148)$

$= 148(112) + 75(-221)$

$= 148(37 - 75) + 75(-73 + 148)$

$= 148(-38) + 75(75)$

Prop- that Outputs d, x, and y of the Extended Euclidean Algm. Satisfy $d = \gcd(a,b)$ and $d = ax + by$.

Proof- We first point out that throughout the algorithm, any of the length-3 vectors $Z = U, V,$ or W always corresponds to a valid equation:

$$Z(1) = a\,Z(2) + b\,Z(3),$$ where $Z = [Z(1), Z(2), Z(3)]$

To see this, note first that it is clearly true for the initial vectors $U = [a, 1, 0]$ and $V = [b, 0, 1]$. (for example, for $Z = U$, the equation becomes

$$a = a \cdot 1 + b \cdot 0$$)

All other vectors created or updated in the algm. are either taken to be a previously constructed vector or (in the case of a W vector) taken as a vector of the form $U + \alpha V$, where α is an integer.

It suffices to show if the vectors U and V both correspond to a valid equation with the above scheme, then so will be the vector $U + \alpha V$.

Indeed, from the corresponding equations for U and V: $U(1) = aU(2) + bU(3)$, $V(1) = aV(2) + bV(3)$

Then $U(1) + \alpha V(1) = a[U(2) + \alpha V(2)] + b[U(3) + \alpha V(3)]$,

which is the (valid) equation corresponding to the vector $U + \alpha V$.

With this being done, it now suffices to show that the algm. eventually terminates, & when it does, we have (the final value)

$$U(1) = \gcd(a, b).$$

As in the proof of the Euclidean Algorithm, if we set $r_0 = b$ and $r_{-1} = a$, the Euclidean Algm. can be expressed as successive applications of the division algm., where each one defines the next element of the remainder sequence:

$$r_{i-1} = q_i r_i + r_{i+1} \quad (i = 0, 1, 2, \cdots, n).$$

Recall that the sequence of remainders is strictly decreasing & the final non-zero remainder (r_n) is $\gcd(a, b)$.

If we look at the first component of the recursive formula of the Extended Euclidean algm.,

i.e. $W(1) = U(1) - \left\lfloor \frac{U(1)}{V(1)} \right\rfloor V(1)$,

we see that $W(1)$ is simply the remainder when division algm. is applied to the integer division of $U(1)$ by $V(1)$.

Since U(1) starts off at a, V(1) starts off at b, and at each iteration, U(1) is updated to V(1) and V(1) to (the new remainder) W(1), we see that at the i-th iteration of the Extended Euclidean algm., W(1) is exactly the value of the new remainder in the i-th iteration of the Euclidean algm.

~~It follows that the value of the new remainder in the i-th iteration~~

It follows that the values of V(1) are strictly decreasing integers (so the algm. terminates) whose last non-zero value is gcd(a,b), as claimed.

Note.

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

$$d = ax + by$$

if $d = 1$

To find $\bar{a}^1$ mod b.

$$1 = ax + by$$

$$\Rightarrow \bar{a}^1 = x \bmod b$$

Modular inverse in $\mathbb{Z}_b$.

Algorithms in $\mathbb{Z}_n$

Computing multiplicative inverse in $\mathbb{Z}_n$

Input: $a \in \mathbb{Z}_n$

Output: $a^{-1} \bmod n$, provided that it exists.

1. Use the Extended Euclidean algm. to find integers x and y such that $ax + ny = d$, where $d = \gcd(a, n)$.
2. If $d > 1$, then $a^{-1} \bmod n$ does not exist.

   Otherwise return (x).

Repeated square-and-multiply algm. for exponentiation in $\mathbb{Z}_n$

Input: $a \in \mathbb{Z}_n$, and integer $0 \le k < n$ whose binary representation is $k = \sum_{i=0}^{t} k_i 2^i$, $k_i \in \{0, 1\}$.

Output: $a^k \bmod n$

$$\left[a^k = \prod_{i=0}^{t} a^{k_i 2^i} = (a^{2^0})^{k_0} (a^{2^1})^{k_1} \cdots (a^{2^t})^{k_t} \right]$$

1. Set $b = 1$. If $k = 0$ then return (b)
2. Set $A = a$
3. If $k_0 = 1$ then Set $b = a$
4. for i from 1 to t do the following:
   - set $A \leftarrow A^2 \bmod n$
   - If $k_i = 1$ then Set $b \leftarrow A \cdot b \bmod n$
5. Return (b).

Exercise: Compute $9726^{3533} \bmod 11413$. $(= 5761)$

$3533 = 110111001101$ (bits $k_{11} \dots k_0$; $k_3 k_2$; $k_8 k_7 k_6$; k_0)

$A = 9726 \bmod 11413$.

Computation of $5^{596} \bmod 1237$

i	k_i	A	b
0	0	5	1
1	0	25	1
2	1	625	625
3	0	681	625
4	1	1011	67
5	0	369	67
6	1	421	1059
7	0	779	1059
8	0	947	1059
9	1	925	1013.

Class Test - 6th. Sep., 2016
Assignment-1 - " "

~~6th. Sep 2018~~
~~Assignment-1~~ "

Example:

Compute $2^{1452} \bmod 19$

Fast Modular Exponentiation:

$2^2 \equiv 4 \pmod{19}$ → continue squaring both sides until the exponent exceeds at least half of the desired exponent.

$2^4 \equiv 4^2 \equiv 16$

$2^8 \equiv 16^2 \equiv 256 \equiv 9$

$2^{16} \equiv 9^2 \equiv 81 \equiv 5$

$2^{32} \equiv 6$

$2^{64} \equiv 17$

$2^{128} \equiv 4$

$2^{256} \equiv 16$

$2^{512} \equiv 9$

$2^{1024} \equiv 5$.

$12 = 2^3 + 2^2$

$2^{12} = 2^8 \cdot 2^4$

$= 16 \cdot 9$

$1452 \sim [10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1\ 0]$

$[1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0]$ (base 2).

$1452 = 1024 + 256 + 128 + 32 + 8 + 4$

$2^{1452} = 2^{1024} \times 2^{256} \times 2^{128} \times 2^{32} \times 2^8 \times 2^4$.

$\equiv 5 \times 16 \times 4 \times 6 \times 9 \times 16$

$\equiv 11 \pmod{19}$

19 | 144 | 7
133
11

Using Fermat's Little Theorem:

$p \rightarrow$ prime
$\gcd(a, p) = 1$
then $a^{p-1} \equiv 1 \pmod{p}$

19 → prime $\quad \gcd(2, 19) = 1 \Rightarrow 2^{18} \equiv 1 \pmod{p}$

$\therefore 1452 = 18 \times 80 + 12$ (by division algm)

$\therefore 2^{1452} \equiv (2^{18})^{80} \times 2^{12} \equiv 1^{80} \times 16 \times 9 \equiv 11 \pmod{19}$

Exercise: Compute $18^{802} \pmod{29}$, using each of the two methods shown above.

Example: Make use of Euler's theorem to perform each of the following tasks:

(a) Compute $18^{2551} \pmod{25}$

(b) Find the last (one's) digit of the integer 13^{2017}

↓ this integer has 2296 digits.

Soln

$$\gcd(18, 25) = 1$$

$$\phi(25) = \phi(5^2)$$

$$= 25\left(1 - \frac{1}{5}\right) = 25 \times \frac{4}{5} = 20$$

[$\gcd(a,m) = 1$, $m > 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$

$\therefore$ By Euler's Theorem, $18^{20} \equiv 1 \pmod{25}$.

$$2551 = 127 \times 20 + 11$$

$$\therefore 18^{2551} \equiv (18^{20})^{127} \cdot 18^{11} \pmod{25}$$

$$\equiv 18^{11} \pmod{25}$$

$$\equiv 18 \times 24 \pmod{25}$$

$$\equiv 7 \pmod{25}.$$

$18 \equiv 18$

$18^2 \equiv 24$

$18^4 \equiv 1$

$18^8 \equiv 1$

$1+2+0+8$

$$\begin{array}{r} 18\cdots \\ 18 \\ \hline 144 \\ 18\times \\ \hline 324 \\ 25 \\ \hline 74 \\ 50 \\ \hline 24 \end{array} \quad 25\overline{)324}\,|12$$

4 3 2 1 0

$11 \sim 1\ 0\ 1\ 1$

$11 = 2^3 + 2 + 1$

$18^{11} = (18)(18)^2(18)^{2^3}$

$18 \quad 24$

$$\begin{array}{r} 24\cdots \\ 18 \\ \hline 432 \\ 25 \\ \hline 182 \\ 175 \\ \hline 7 \end{array} \quad 25\overline{)}\,17$$

$$\begin{array}{r} 24 \\ 24 \\ \hline 96 \\ 48\times \\ \hline 576 \\ 50 \\ \hline 76 \\ 75 \\ \hline 1 \end{array} \quad 25\overline{)}\,23$$

(b) Last digit of the integer 13^{2017}

↓

$13^{2017} \pmod{10}$

$\gcd(13, 10) = 1$, $\phi(10) = \phi(5 \times 2) = \phi(5) \times \phi(2)$
$= 4 \times 1 = 4$

By Euler's Theorem, $13^{\phi(10)} = 13^4 \equiv 1 \pmod{10}$.

$2017 = 504 \times 4 + 1$

$13^{2017} \equiv (13^4)^{504} \times 13 \pmod{10}$

$\equiv 1 \times 13 \pmod{10}$

$\equiv 3 \pmod{10}$

∴ Last digit is 3.

Exercise

(a) Compute $7^{8486} \pmod{58}$

(b) Find the last three digits of the integer 13^{2017}.

↓ mod 1000

Ans: 993

Drawback

Evaluating $\phi(n)$ requires the prime factorization of n → very hard problem, no efficient algorithm exists.
→ Base of RSA cryptosystem.

Modular Orders of Invertible Modular Integers

Defn For integers $1 \le a < n$, with a & n relatively prime, we define **order of a relative to n** (or order of a mod n), denoted by $\text{ord}_n(a)$, is defined to be the smallest positive exponent k for which

$$a^k \equiv 1 \pmod{n}.$$

By Euler's Theorem, $\text{ord}_n(a) \le \phi(n)$.

Example

(a) Compute the orders mod n of all positive integers less than (and relatively prime to) $n = 7$.

(b) Do the same for $n = 8$

$\phi(n) = \phi(7) = 7 - 1 = 6$

$\mathbb{Z}_7^*$ is not a prime order group.

Powers (mod 7) of integers relatively prime to $n = 7$

	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
$a=1$	[1]	1	1	1	1	1
$a=2$	2	4	[1]	2	4	1
$a=3$	3	2	6	4	5	[1] →
$a=4$	4	2	[1]	4	2	1
$a=5$	5	4	6	2	3	[1] →
$a=6$	6	[1]	6	1	6	1

$a = 3, 5 \rightarrow$ two generators.

# of generators $\rightarrow \phi(\phi(7))$

$= \phi(6)$

$= \phi(3 \times 2)$

$= 2 \times 1 = 2$

powers (mod 8) of Integers Relatively prime to n = 8

$\phi(8) = \phi(2^3) = 8(1-\frac{1}{2}) = 4$

$a^k \pmod 8$

	k=1	k=2	k=3	k=4
a=1	[1]	1	1	1
a=3	3	[1]	3	1
a=5	5	[1]	5	1
a=7	7	[1]	7	1

* not cyclic as no elt of order $\phi(8)=4$

$21|85|4$ $\frac{84}{1}$

$21|160|$

$21|169|4$ $\frac{84}{16}$

$21|69|3$ $\frac{63}{1}$

$21|80|3$ $\frac{63}{17}$

powers (mod 21) of Integers Relatively prime to n = 21

$\phi(21) = \phi(7\times3) = \phi(7)\phi(3) = 6\times2 = 12$

$a^k \pmod{21}$

	k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9	k=10	k=11	k=12
a=1	[1]	1	1	1	1	1	1	1	1	1	1	1
a=2	2	4	8	16	11	[1]	2	4	8	16	11	1
a=4	4	16	[1]	4	16	1	4	16	1	4	16	1
a=5	5	4	20	16	17	[1]	5	4	20	16	17	1
a=8	8	[1]	8	1	8	1	8	1	8	1	8	1
a=10	10	16				[1]						
a=11						[1]						
a=13		[1]										
a=16			[1]									
a=17						[1]						
a=19						[1]						
a=20	[1]											

* not cyclic as no elt of order $\phi(21)=12$

Fact Suppose that a and $n > 1$ are relatively prime positive integers.

(a) If k is a positive integer with $a^k \equiv 1 \pmod{n}$, then $\text{ord}_n(a) \mid k$.

(b) $\text{ord}_n(a) \mid \phi(n)$

(c) If i and j are non-negative integers, then $a^i \equiv a^j \pmod{n}$ iff $i \equiv j \pmod{\text{ord}_n(a)}$. i.e. when working mod n, exponents can be reduced mod $\text{ord}_n(a)$

proof-

(a) By division algm,

$$k = q\,\text{ord}_n(a) + r, \quad 0 \le r < \text{ord}_n(a), \quad q, r \in \mathbb{Z}$$

$$\therefore a^k \equiv 1 \pmod{n} \Rightarrow a^{q\,\text{ord}_n(a) + r} \equiv 1 \pmod{n}$$

$$\text{i.e.} \quad \left(a^{\text{ord}_n(a)}\right)^q a^r \equiv 1 \pmod{n}$$

$$\text{i.e.} \quad a^r \equiv 1 \pmod{n}$$

when $r < \text{ord}_n(a)$

$\Rightarrow$ contradiction unless $r = 0$

$\therefore k = q\,\text{ord}_n(a)$

i.e. $\text{ord}_n(a) \mid k$.

(b) By Euler's Theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$.

$\therefore$ By (a), $\text{ord}_n(a) \mid \phi(n)$.

(c) Let $a^i \equiv a^j \pmod n$ & $i \geq j$ (switching the roles of i & j if necessary)

(1) $\because \gcd(a, n) = 1$

$\therefore$ multiplicative inverse of a ($\bar{a}^1$) exist mod n.

(1) $\times (\bar{a}^1)^j$

$$a^i (\bar{a}^1)^j \equiv a^j (\bar{a}^1)^j \pmod n$$

i.e. $a^{i-j} \equiv 1 \pmod n$ as $\gcd(a, n) = 1$

$\therefore$ By part (a)

$$\text{ord}_n(a) \mid i-j$$

i.e. $i \equiv j \bmod (\text{ord}_n(a))$.

Conversely, Let $i \equiv j \bmod (\text{ord}_n(a))$ & $i \geq j$

$\therefore i - j = q \cdot \text{ord}_n(a)$

or $i = j + q \cdot \text{ord}_n(a)$, $q \in \mathbb{Z}$ (non negative)

$$\therefore a^i \equiv a^{j + q \cdot \text{ord}_n(a)} \equiv a^j \left(a^{\text{ord}_n(a)}\right)^q \equiv a^j \cdot 1^q$$

$$\equiv a^j \pmod n$$

Order of Powers formula

Theorem:
If $a, j, n > 1$ are positive integers, with a relatively prime to n, then

$$\text{ord}_n(a^j) = \frac{\text{ord}_n(a)}{\gcd\left(j, \text{ord}_n(a)\right)}.$$

$\Rightarrow$ a is a primitive root mod n & $=1$ means a^j is also a primitive root mod n.

~~Proof:~~

Corollary: If g is a primitive root $(\text{mod } n)$, then the other primitive roots $(\text{mod } n)$ are the same as the modular powers $g^j \ (\text{mod } n)$, as j runs through all of the positive integers less than & relatively prime to $\phi(n) = \text{ord}_n(g)$.

Proof of the theorem

Let $m = \text{ord}_n(a)$ & $l = \text{ord}_n(a^j)$.

$a^{jl} \equiv 1 \ (\text{mod } n)$ iff $m \mid jl$ (by def^n of m)

But l is the least +ve int. ~~for which~~ s.t. $a^{jl} \equiv 1 \ (\text{mod } n)$ (by def^n of l)

$\therefore$ $jl = \text{lcm}(m, j)$ Why?

$$= \frac{mj}{\gcd(m, j)}$$

$\Rightarrow$ $l = \frac{m}{\gcd(m, j)}$ $\Rightarrow$ $\text{ord}_n(a^j) = \frac{\text{ord}_n(a)}{\gcd\left(j, \text{ord}_n(a)\right)}$

$m \rightarrow$ a multiple of jl
$j \rightarrow$ a multiple of jl

~~lcm(j,m) | jl~~
~~jl ≠ lcm(j,m)~~
~~Then~~

Example: If possible, do each of the following:

(a) Compute $\operatorname{ord}_{59}(7)$.

(b) find an integer between 1 and 59 whose mod 59 order is 22.

(c) find a primitive root of 59.

(d) find an exponent j s.t. $g^j \equiv 7 \pmod{59}$, where g is the primitive root that was found in part (c).

Sol^n:

(a) $\operatorname{ord}_{59}(7) \mid \phi(59)$

$\phi(59) = 59-1 = 58 = 2 \times 29$

$\therefore \operatorname{ord}_{59}(7)$ is either 2 or 29 or 59.

Compute $7^2 \equiv 49 \pmod{59}$

$7^{29} = 7^{16} \times 7^8 \times 7^4 \times 7$

$\equiv 15 \times 29 \times 41 \times 7$

$\equiv 15 \times 29 \times 51$

$\equiv 57$

$\equiv 57 \times 29$

$\equiv 1 \pmod{59}$.

$\therefore \operatorname{ord}_{59}(7) = 29$.

(b) $22 \times 58 = \phi(59) \Rightarrow$ no integer with order 22 mod 59.

$29 = 2^4 + 2^3 + 2^2 + 2^0$

$= 16 + 8 + 4 + 1$

$7^2 = 49$

$7^4 = 41$

$7^8 = 29$

$7^{16} = 15$

(c) ∵ 59 is prime

∴ it will have $\phi(\phi(59)) = \phi(58) = 28$ primitive roots

To find a primitive root of 59

apply simple Brute force search starting with

$a = 2$ $\qquad \phi(59) = 58 = 2 \times 29$

find powers of $2^2, 2^{29}$; if neither congruent to 1 mod 58

$a = 2$ is a primitive root

else $a \to a+1 = 3$.

Continue this process until we find a primitive root

$2^2 \equiv 4 \pmod{59}$

$2^{29} \equiv 2^{16} \times 2^8 \times 2^4 \times 2$

$\equiv 46 \times 20 \times 16 \times 2$

$= 46 \times 20 \times 16 \times 2$

$\equiv 46 \times 50$

$\equiv 58 \pmod{29}$

$29 = 2^4 + 2^3 + 2^2 + 2^0$

$= 16 + 8 + 4 + 1$

$2^2 \equiv 4$

$2^4 \equiv 16$

$2^8 \equiv 20$

$2^{16} \equiv 46$

59 | 2300 | 38
177
530
472
58

59 | 250 | 4
236
14

59 | 256 | 4
236
20

59 | 400 | 7
59
41

59 | 400 | 7
295
25

59 | 1025 | 17
59
445
413
32

59 | 640 | 11
59
50

59 | 100 | 7
59
5

59 | 140 | 16
59
359
46

(d) This is discrete logarithm question.

$\because$ $g=2$ is a primitive root, $\text{ord}_{59}(2) = \phi(59) = 58$

$$\therefore \text{ord}_{59}(2^j) = \frac{\text{ord}_{59}(2)}{\gcd\left(j, \text{ord}_{59}(2)\right)} = \frac{2\times 29}{\gcd(j, 2\times 29)}$$

To find j s.t. $2^j \equiv 7 \pmod{59}$

Since $\text{ord}_{59}(7) = 29$

$\therefore$ j must be even, $j = 2k$

By Brut-force approach, compute even powers of 2

$2^2, 2^4, 2^6, 2^8, \ldots \pmod{59}$

& check $2^{18} \equiv 7 \pmod{59}$.

desired dL is $j = 18$.

Exercise Sil^n

(a) How many primitive roots does $n = 334$ have?

(b) What is the smallest ~~positive~~ primitive root?

(c) How many integers mod 334 have order equal to 2?

RSA Execute.

# of primitive $= \phi(\phi(59)) = \phi(58) = \phi(2)\phi(29) = 1\times 28 = 28$.

$\text{ord}_{59}(x) = 2 = \text{ord}_{59}(2^j) = \frac{58}{\gcd(j,58)}$, $1 \le j \le 58$

$\Rightarrow \gcd(j,58) = 29 = \frac{2\times 29}{}$

$\therefore j = 29, 3\times 29$

$\Rightarrow \gcd(j, \frac{2\times 29}{58}) = \frac{58}{2} = 29$

$\Rightarrow j = 2, 4, 6, 8, 10, 12, \ldots$ $1 \le j \le 58$

$\Rightarrow j = 29, 3\times 29$

~~to be integer, must be even.~~

$\gcd(j, 2\times 29) = 58 / \text{ord}_{59}(2^j) = \frac{58}{\text{ord}_{59}(7)} = \frac{58}{29} = 2$

$\Rightarrow j$ must be even

$\text{ord}_{59}(2^j) = \frac{2\times 29}{\gcd(2k, 2\times 29)} = \frac{2\times 29}{2} = 29$.

Find the # of elements of order 29

$\text{ord}_{59}(x) = 29$, $1 \le j \le 58$

Let $x = 2^j$, $\text{ord}_{59}(2^j) = \frac{\text{ord}_{59}(2)}{\gcd(j,58)}$

$\therefore \frac{58}{\gcd(j,58)} = 29$

Example:

a) Verify that $g=3$ is a primitive root of 223.

b) How many integers mod 223 have order 6?
If such elements exist, find one.

c) How many integers mod 223 have order 74?
If such element exist, find one.

d) How many integers mod 223 have order 10?
If such element exist, find one.

Sol^n:

~~(a) Verify that $3^{\phi(223)} \equiv 1 \pmod{223}$ but $3^2, 3^3, \ldots$~~

a) $\phi(223) = 222 = 2 \times 3 \times 37$.

check that ~~$3^2, 3^3, 3^{37}, 3^6, 3^{2\times 37}, 3^{3\times 37}$~~

$\not\equiv 1 \pmod{223}$.

$\therefore \; 3^{222} \equiv 1 \pmod{223}$.

d) $10 \nmid 222 \Rightarrow$ no element of order 10 modulo 223.

~~(b) 3 is a primitive root modulo 223.~~

~~Find $\text{ord}_{223}(x) = 6$~~

$6, 74 \mid 222 \Rightarrow$ There may exist elements of order 6 & 74 modulo 223.

(b) $\#x \in \mathbb{Z}_{223}$ s.t. $\operatorname{ord}_{223}(x) = 6$.

$\therefore$ 3 is a primitive root modulo 223

$\therefore x = 3^j, \quad 1 \le j \le 222.$

By order of powers formula,

$$\operatorname{ord}_{223}(3^j) = \frac{\operatorname{ord}_{223}(3)}{\gcd(j, \operatorname{ord}_{223}(3))}.$$

$$= \frac{222}{\gcd(j, 222)} = 6$$

$$\Rightarrow \gcd(j, 222) = \frac{222}{6} = 37.$$

$222 = 2 \times 3 \times 37$

$1 \le j \le 222.$

$j = 37, 5 \cdot 37,$ ~~$7 \cdot 37 = 259 > 222$~~

$\therefore$ There are 2 elements of order 6 modulo 223 namely, $3^{37} \bmod 223$ & $3^{5 \cdot 37} \bmod 223$.

(c) Exercise $\operatorname{ord}_{223}(x) = 74$

$1 \to 74 \to$ add mul. 37.

$\gcd(j, 222) = \frac{222}{74} = 3, \quad 1 \le j \le 222$ (all odd)

$j \to$ exclude 3×37: $1 \cdot 3, 3 \cdot 3, 5 \cdot 3, 7 \cdot 3, 9 \cdot 3, 11 \cdot 3, 13 \cdot 3, 15 \cdot 3, 17 \cdot 3, 19 \cdot 3, 21 \cdot 3, 23 \cdot 3, \ldots 73 \cdot 3$ $\to$ Total 36.

order 74 elements modulo 223 are 3^j, $j = 3, 9, 15, \ldots$

Solving the Single linear Congruence

$ax \equiv c \pmod m$, $d = \gcd(a, m)$, $d \mid c$. —— (1)

1. No soln if $d \nmid c$
2. Solve the modified congruence

$$\frac{a}{d} y \equiv \frac{c}{d} \pmod{\frac{m}{d}} \quad \text{—— (2)}$$

which has a unique soln: y_0 as $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$.

3. The d solns of the original congruence are

$y_0 + i\frac{m}{d}$, $0 \le i \le d-1$.

$\pmod m$

Proof of Correctness

Claim 1 d solns indicated by the algm. actually solve the original congruence (1)

proof. $\frac{a}{d} y_0 \equiv \frac{c}{d} \pmod{\frac{m}{d}}$

$\Rightarrow \frac{m}{d} \mid \left[\frac{a}{d} y_0 - \frac{c}{d}\right]$

$\Rightarrow m \mid (ay_0 - c) \Rightarrow ay_0 \equiv c \pmod m$

$\Rightarrow y_0$ is a soln.

$d = \gcd(a, m) \Rightarrow d \mid a$

$\frac{a}{d}\left(y_0 + \frac{im}{d}\right)$

$\equiv \frac{a}{d} y_0 + \frac{aim}{d}$

$\equiv c \pmod m$

$\Rightarrow y_0 + \frac{im}{d}$ is a soln

$1 \le i \le d-1$

Claim There are no other soln^s $\pmod m$.

proof:

Note No other soln^s of (1) of the form

$$y_0 + \frac{im}{d} \pmod m,$$

$i \in \mathbb{Z}$;

other than d soln^s indicated by the alg^m

Because for any integer $i \in \mathbb{Z}$, if $r = i \bmod d$,

then $y_0 + \frac{im}{d} \equiv y_0 + \frac{rm}{d} \pmod m$

To prove (1) has no soln^n other than these.

Suppose z_0 is a soln^n of (1)

$\therefore az_0 \equiv c \pmod m$ — (2).

$\therefore \exists$ unique int. i s.t.

$$y_0 + \frac{im}{d} \leq z_0 < y_0 + \frac{(i+1)m}{d}$$

$$\Rightarrow \frac{im}{d} \leq z_0 - y_0 < \frac{(i+1)m}{d}.$$

$$\Rightarrow z_0 \not\equiv y_0 \pmod m$$

(2)

$\Rightarrow \frac{a}{d} z_0 \equiv \frac{c}{d} \pmod{\frac{m}{d}}$ which contradicts the fact that y_0 is the unique soln^n of this congruence (2).

Chinese Remainder Theorem

① $\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$

$n_1, n_2, \cdots, n_k$ pairwise relatively prime

↳ unique sol^n.

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i \pmod{n} \quad \text{—— ②}$$

$a_i N_i (N_i^{-1} \bmod n_i) \pmod{n}$

↓

$N_i = \frac{n}{n_i}$

where $n = n_1 n_2 \cdots n_k$

$N_i = \frac{n}{n_i}$

$M_i = N_i^{-1} \bmod n_i$

proof. (Existence)

$\gcd(N_i, n_i) = 1, \quad 1 \le i \le k.$

$\therefore \exists$ unique sol^n M_i of the congruence

$$N_i M_i \equiv 1 \pmod{n_i}.$$

Claim: $x = \sum_{i=1}^{k} a_i N_i M_i$ is a simultaneous sol^n. of eqn. ②:

Now ~~$N_i \bmod n_j$~~ $N_i \equiv 0 \pmod{n_j}$ unless $i = j$

$\therefore x = a_1 N_1 M_1 + a_2 N_2 M_2 + \cdots + a_j N_j M_j + \cdots + a_k N_k M_k$

$\equiv \cancel{0 + 0 + \cdots + a_j N_j M_j} \pmod{n_j}$

$\equiv a_j N_j M_j \pmod{n_j} \equiv a_j \cdot 1 \equiv a_j \pmod{n_j}$

Uniqueness

x' → another simultaneous soln. of equn. (1).

$\therefore \forall i,\ 1 \le i \le k$, $\quad x \equiv a_i \equiv x' \pmod{n_i}$.

$\Rightarrow \quad n_i \mid x - x'$

Since the n_i's are pairwise relatively prime, their product

$n = n_1 n_2 \cdots n_k$ also divides $x - x'$

i.e. $\quad n \mid x - x'$

i.e. $\quad x \equiv x' \pmod{n}$.