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 $\mathbb{Z}_b$.

Use of Extended Euclidean Algm. to solve linear Diophantine equn.

- $ax+by=c$ — (1) a, b, c integers, at least one of a, b non-zero.

  ↓ has a soln.

  iff

  $\gcd(a,b) \mid c$. (Apply Extended Euclidean algm to get $d = \gcd(a,b) = au + bv$)

  x_0, y_0 found using u, v this algm

  ↓

  a particular soln. of (1). Can be obtained using u, v.

  ↓

  say x_0, y_0

- ~~All Soln~~

$d = au + bv$.

$d \mid c \Rightarrow c = kd$.

$\therefore kd = aku + bkv$.

i.e. $c = a(ku) + b(kv)$

$= ax_0 + by_0$.

$\Rightarrow (x_0, y_0)$ is a particular soln. to (1).

- **All solns.**

$$x = x_0 + \frac{b}{\gcd(a,b)} t$$

$$y = y_0 - \frac{a}{\gcd(a,b)} t$$

} with t arbitrary integer.

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.

(Inverse in $\mathbb{Z}_n$)

Theorem: Let $a \in \mathbb{Z}_n$. Then a is invertible iff $\gcd(a,n) = 1$. In particular, all non-zero elements of $\mathbb{Z}_n$ are invertible precisely when $n = p$ is prime.

Proof: If $\gcd(a,n) = 1$, then there exist integers x, y s.t. $1 = ax + ny$.

Rewriting this as $1 - ax = ny$, we see that $n \mid (1 - ax)$, and so $ax \equiv 1 \pmod{n}$.

This implies (resetting x to be its mod n representative between 1 & $n-1$) that $x = \bar{a}^{-1}$ in $\mathbb{Z}_n$.

Conversely, if a has an inverse $\bar{a}^{-1}$ in $\mathbb{Z}_n$, then

$$a\bar{a}^{-1} \equiv 1 \pmod{n},$$

or $n \mid (1 - a\bar{a}^{-1})$

It follows that $1 - a\bar{a}^{-1} = nk$ or $nk + a\bar{a}^{-1} = 1$, $\quad bx + cy$

for some $k \in \mathbb{Z}$.

$\Rightarrow \gcd(n,a) = 1$, because any (prime) factor of a and n would also necessarily have to be a (prime) factor of 1 (which has no prime factor).

[$a \mid b$, $a \mid c \Rightarrow a \mid (bx + cy)$ for any ints. x & y]

i.e. common factor of b, c is also a factor of $bx + cy$

The last statement of the theorem ~~easily~~ easily follows from the criterion since any prime number p is relatively prime to all positive integers that are less than p, i.e., to all non-zero elements in Z_p.

Solving single linear congruence.

CRT.

Order of powers formula.

RSA Exercise

Poimality Testing — Fermat's
— Miller-Rabin
— Solovay-Strassen (Quadratic residues).

→ proving only Compositeness
→ not capable of proving that a number is prime.

Fermat's Little Theorem

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.

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

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

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

$2^{32} \equiv 6$

$2^{64} \equiv 17$

$2^{128} \equiv 4$

$2^{256} \equiv 16$

$2^{512} \equiv 9$

$2^{1024} \equiv 5$.

$12 = 2^3 + 2^2$

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

$= 16 \cdot 9$

$1452 \sim [1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0]$ (base 2)

(10 9 8 7 6 5 4 3 2 1 0)

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

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

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

$\equiv 11 \pmod{19}$

19 | 144 | 7
133
11

Using Fermat's Little Theorem:

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

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

$\therefore 1452 = 18 \times 80 + 12$ (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.

• Security : Difficulty of factoring large integer.

RSA

$n = pq$

$\mathcal{P} = \mathcal{C} = Z_n$

$K = (n, p, q, a, b)$ — n, b public; p, q, a private.

$ab \equiv 1 \pmod{\varphi(n)}$

Security is based on factoring is hard

if someone can factor $\varphi(n)$, then no security.

$e_K(x) = x^b \bmod n$

$d_K(y) = y^a \bmod n$.

$x, y \in Z_n$.

$d_K(e_K(x)) = d_K(e_K(x))^a$

$= x^{ab}$.

no one other than B knows p, q, so $\varphi(n)$, so a

factrization of n (the trapdoor information)

$x \in Z_n$, $y = x^b \bmod n$

A → B

Secret a, p, q.

n, b.

$y^a \bmod n$

$= x^{ab} \bmod n$

$= x^1 \bmod n$

- B generates two large primes, $p \neq q$ → how?
- B Computes $n = pq$ & $\varphi(n) = (p-1)(q-1)$
- B Chooses randomly b, $1 < b < \varphi(n)$ s.t. $\gcd(b, \varphi(n)) = 1$ → check it using the Euclidean algo.
- B Computes $a = b^{-1} \bmod \varphi(n)$ using Extended Euclidean algo.
- B Publishes n, b. Secret key of B is p, q, a.

Euclidean algo

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?

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

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

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

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

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

ElGamal Encryption Scheme in Z_p^*.

Security: the difficulty of the discrete logarithm problem for finite fields

DL problem in Z_p: given p, α, β, p prime

$Z_p^* = \langle \alpha \rangle$

$\beta \in Z_p^*$

to find $a \in Z$, $0 \le a \le p-2$ s.t.

$$\alpha^a \equiv \beta \pmod p.$$

$p \to$ prime s.t. DLP is intractable in Z_p.

$Z_p^* = \langle \alpha \rangle$.

$\mathcal{P} = Z_p^*$, $\mathcal{C} = Z_p^* \times Z_p^*$, $\mathcal{K} = \{ (p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p \}$

(a: secret; p, α, β: public)

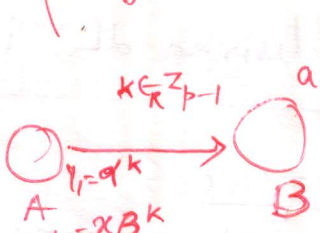
Encryption: $K = (p, \alpha, a, \beta)$.

choose randomly $k \in Z_{p-1}$ & define

$e_K(x, k) = (y_1, y_2)$

where $y_1 = \alpha^k \bmod p$

$y_2 = x \beta^k \bmod p$



Decryption: For $(y_1, y_2) \in \mathcal{C}$,

$$d_K(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p$$

$$x \beta^k \cdot (\alpha^{ak})^{-1} \equiv x \alpha^{ka} (\alpha^{ka})^{-1} \equiv x \pmod p$$

$y_2 (y_1^a)^{-1} = x \beta^k (\alpha^{ka})^{-1} = x \alpha^{ka} (\alpha^{ka})^{-1} = x.$

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, $j = 3, 9, 15, \ldots$