ALGEBRA and NUMBER THEORY INTRODUCTION

APPENDIX

In this appendix several simple and basic concepts and methods of algebra and number theory are summarized.

Basic algebraic structures, such as groups, rings and fields play key role in theory of error-correcting codes and in cryptography.

The number theory concepts, methods and results introduced in the following play an important role in modern considerations concerning cryptography, cryptographic protocols and randomness.

The key concept is that of primality. The key methods are based on randomized algorithms.

GROUPS

A **group** G is a set of elements and an operation, call it *, with the following properties:

- G is closed under *; that is if $a, b \in G$, so is $a * b$.
- The operation * is associative $(a*(b*c) = (a*b)*c$, for any $a, b, c \in G$.
- G has an identity e element so that $e * a = a * e = a$ for any $a \in G$.
- Every element $a \in G$ has an inverse $a^{-1} \in G$, so that $a * a^{-1} = a^{-1} * a = e$.

group G is called **Abelian** if the operation $*$ is commutative $(a*b = b*a$ for any $a, b \in G)$.

Example Which of the following sets is an (Abelian) group:

- The set of real numbers with $*$ being: (a) addition; (b) multiplication.
- The set of matrices of degree n and an operations (a) addition; (b) multiplication.
- What happens if we consider only matrices with determinants not equal zero?

RINGS and FIELDS

A **ring** R is a set with two operations $+$ (addition) and $\cdot$ (multiplication) , with the following properties:

- R is closed under $+$ and $\cdot$.
- R is an Abelian group under $+$ (with the unity element for addition called **zero**).
- The associative law for multiplication holds.
- R has an identity element 1 for multiplication
- The distributive law holds $(a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.

ring is called **commutative** if multiplication is commutative

A **field** F is a set with two operations $+$ (addition) and $\cdot$ (multiplication) , with the following properties:

- F is a commutative ring.
- Non-zero elements of F form an Abelian group with respect to multiplication.

A non-zero element g is a **primitive element** of a field F if all non-zero elements of F are powers of g.

FINITE FIELDS

Finite field are very well understood.

Theorem If p is a prime, then the integers $\mathrm{mod} p$, $GF(p)$, constitute a field. Every finite field F contains a subfield that is $GF(p)$, up to relaabeling, for some prime p and $p \cdot \alpha = 0$ for every $\alpha \in F$.

If a field F contains the prime field $GF(p)$, then p is called the **characteristic** of F.

Theorem (1) Every finite field F has p^m elements for some prime p and some m.

(2) For any prime p and any integer m there is a unique (up to isomorphism) field of p^m elements $GF(p^m)$.

(3) If $f(x)$ is an irreducible polynomial of degree m in $F_p[x]$, then the set of polynomials in $F_p[x]$ with additions and multiplications modulo $f(x)$ is a field with p^m elements.

Ceiling and floor functions

Flour $\lfloor x \rfloor$ – the largest integer $\leq x$
Ceiling $\lceil x \rceil$ – the smallest integer $\geq x$

Example $\lfloor 3.14 \rfloor = 3 = \lfloor 3.75 \rfloor \quad \lfloor -3.14 \rfloor = -4 = \lfloor -3.75 \rfloor$
$\lceil 3.14 \rceil = 4 = \lceil 3.75 \rceil \quad \lceil -3.14 \rceil = -3 = \lceil -3.75 \rceil$

Exercise $\lceil x \rceil - \lfloor x \rfloor = ?$

Modulo operations

The remainder if n is divided by m is defined by

$$n \mod m = \begin{cases} n - m \left\lfloor \frac{n}{m} \right\rfloor & m \neq 0 \\ 0 & m = 0 \end{cases}$$

Example $7 \mod 5 = 2 \qquad 7 \mod -5 = 2$
$-7 \mod 5 = 3 \qquad -7 \mod -5 = 3$

Properties • $(a + b) \mod n = ((a \mod n) + (b \mod n)) \mod n$
• $(a \cdot b) \mod n = ((a \mod n) \cdot (b \mod n)) \mod n$
• $a^b \bmod n = (a \bmod n)^b) \bmod n.$

Exercise $3^{123456789} \mod 26 = ?$

EUCLID'S ALGORITHM

to compute $gcd(m, n), 0 \leq m < n$

$$\gcd(0, n) = n \tag{13}$$
$$\gcd(m, n) = \gcd(n \mod m, m) \text{ for } m > 0 \tag{14}$$

Theorem $T(n) = \mathcal{O}(\log n)$ for the number of steps of Euclid's algoritm.

Proof Aftrer the first step arguments are (n_1, m), where

$$n_1 = n \mod m.$$

After the second step arguments are (m_1, n_1), where

$$m_1 = m \mod n_1.$$

Since $a \mod b < \frac{a}{2}$ if $0 < b < a$, we have:

$$n_1 \leq \frac{n}{2}, m_1 \leq \frac{m}{2}.$$

This analysis was made more precisse by E. Lucas (1884) and Lamé (1884), in perhaps the first deeper analysis of algorithms.

Theorem (1) If $n > m \geq 0$, and an application of Euclid's algorithm to arguments m, n results in k recursive steps, then $n \geq F_{k+2}, m \geq F_{k+1}$.
(2) If $n > m \geq 0, m < F_{k+1}$, then the application of Euclid's algorithm to arguments n, m requires less than k steps.

Corollary $T(n) = \Theta(\log n)$ for the number of steps of Euclid's algoritm.

Properties Is there an asymptotycally faster algorithm to compute $\gcd(m, n)$?

Modified Euclid's algorithm

$$\begin{aligned} \gcd(0,n) &= n & (15)\\ \gcd(m,n) &= gcd(m,n-m), 0 < m < n. & (16) \end{aligned}$$

Lemma $T(n) = \Theta(n)$ for the number of steps of the modified Euclid algoritm.

Corollary Modified Euclid's algorithm is of exponential complexity.

Extended Euclid's algorithm

Theorem For all $0 < m < n$ there exist integers x and y such that

$$\gcd(m,n) = xm + yn.$$

Moreover, x and y can be computed in polynomial time.

Proof If $m = 0$, then $x = 0, y = 1$.
If $m > 0$, take $r = n \mod m$ and compute recursively x', y' such that

$$x'm + y'r = \gcd(r,m).$$

Since $r = n - \left\lfloor \frac{n}{m} \right\rfloor m$ we have:

$$\gcd(m,n) = x'm + y'\left(n - \left\lfloor \frac{n}{m} \right\rfloor m\right) = \left(x' + y'\left\lfloor \frac{n}{m} \right\rfloor\right) m + y'n.$$

An extention of Euclid's algorithm, which computes x and y together with $\gcd(m,n)$ is sometimes referred to as **extended Euclid's algorithm**.

Exponentiation

Exponentiation (modular) plays the key role in many cryptosystems. If

$$n = \sum_{i=0}^{k-1} b_i 2^i, \quad b_i \in \{0,1\}$$

then

$$e = a^n = a^{\sum_{i=0}^{k-1} b_i 2^i} = \prod_{i=0}^{k-1} a^{b_i 2^i} = \prod_{i=0}^{k-1} (a^{2^i})^{b_i}$$

Algorithm for exponentiation

begin $e \leftarrow 1$; $p \leftarrow a$;
  for $i \leftarrow 0$ **to** $k-1$
    do if $b_i = 1$ **then** $e \leftarrow e \cdot p$;
      $p \leftarrow p \cdot p$
    od
end

Modular exponentiation: $a^n \mod m = ((a \bmod m)^n) \bmod m$

Modular multiplication: $ab \mod n = ((a \mod n)(b \mod n) \mod n)$

Exercise $3^{1000} \bmod 19 = 16$
$3^{10000} \bmod 13 = 3$
$3^{340} \bmod 11 = 1$
$3^{100} \bmod 79 = 51$

PRIMES

A positive integer $p > 1$ is called **prime** if it has just two divisors: 1 and p.

Fundamental theorem of arithmetic: Each integer n has a unique decomposition

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

where $p_i < p_{i+1}$ are primes and e_i are integers.

How many primes $\Pi(n)$ are there among the first n integers?

Estimations $\Pi(n) \doteq \frac{n}{\ln n}$ (due to Gauss)
Prime number theorem.

$$\Pi(n) = \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + \frac{2!n}{(\ln n)^3} + \frac{3!n}{(\ln n)^4} + \Theta\left(\frac{n}{(\ln n)^6}\right)$$

The largest known prime:1994: $2^{859433} - 1$; (258716 digits)
1996: $2^{1257787} - 1$; (378632 digits)
1997: $2^{2976221} - 1$;

The largest computed value of $\Pi(x)$: $\Pi(10^{18}) = 24739954287860$

How difficult is to determine whether a given integer is prime.

– No polynomial time algorithm for prime recognition is know
– There is a polynomial algorithm for prime recognition provided GRH (Generalized Rieman Hypothesis) holds
– Prime recognition problem is in **ZPP**, in **NP** and it is not known to be **NP**-complete.

Chinese Remainder Theorem

Theorem Let $m_1, \ldots, m_t$ be integers, $\gcd(m_i, m_j) = 1$ if $i \neq j$ and $a_1, \ldots, a_t$ be integers, $0 < a_i < m_i, 1 \leq i \leq t$.
Then the system of congruences

$$x \equiv a_i \pmod{m_i}, 1 \leq i \leq t$$

has the solution

$$x = \sum_{i=1}^{t} a_i M_i N_i \qquad (\star)$$

where

$$M = \prod_{i=1}^{t} m_i, M_i = \frac{M}{M_i}, N_i = M_i^{-1} \bmod m_i$$

and the solution $(\star)$ is unique up to the congruence modulo M.

Corollary Each integer $0 < x < M$ is uniquelly represented by t-tuple: $x \mod m_1, \ldots, x \mod m_t$.

Example If $m_1 = 2, m_2 = 3, m_3 = 5$, then $(1, 0, 2)$ represents 27.

Advantage: With such a modular representation addition, substraction and multiplication can be done componentwise in parallel time.

Euler totient function

$$\Phi(n) = |\mathbb{Z}_n^\star| = |\{m | 1 \leq m \leq n, \gcd(m,n) = 1\}|$$

Basic properties:
- $\Phi(1) = 1$
- $\Phi(p) = p - 1$, if p is a prime;
- $\Phi(p^k) = p^{k-1}(p-1)$, if p is prime, $k > 0$;
- $\Phi(nm) = \Phi(n)\Phi(m)$, if $\gcd(m,n) = 1$;

Theorem Computation of $\Phi(n)$ and factorization of n are computationally polynomially related problems.

Proof (1) If factorization of $n = \prod_{i=1}^{k} p_i^{e_i}$ is known, then

$$\Phi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}$$

is easy to compute.
(2) The opposite assertion will be shown only for the case $n = p_1 p_2$. In such a case

$$\Phi(n) = (p_1 - 1)(p_2 - 1)$$

and

$$p_1 + p_2 = p_1 p_2 + 1 - \Phi(n) = n + 1 - \Phi(n)$$

Given $p_1 + p_2$ and $p_1 p_2$ it is easy to determine p_1 and p_2.
In addition, it holds

$$\frac{\Phi(n)}{n} = \Omega\left(\frac{1}{\log n}\right)$$

Basic theorems

Theorem (Lagrange) If $(H, \circ)$ is a subgroup of a group $(G, \circ)$, then $|H|$ divides $|G|$).

Theorem (Euler's Totient Theorem)

$$n^{\Phi(m)} \equiv 1 \pmod m$$

if $n < m, \gcd(m, n) = 1$

Corollary $n^{-1} \equiv n^{\Phi(m)-1} \pmod{m}$ if $n < m, \gcd(m, n) = 1$

Theorem (Fermat's Little Theorem)

$$a^p \equiv a \pmod p$$

if p is prime.

Proof Theorem is true for $a = 1$. Assume it is true for some a.
By induction

$$(a + 1)^p \equiv a^p + 1 \equiv a + 1 \mod p.$$

Example If $x \equiv y \mod p - 1$, where p is a prime, then $x - y = k(p - 1)$ and therefore for any $a < p$, $a^{x-y} = a^{k(p-1)} \equiv 1 \bmod p$

Discrete square roots and logarithms

Three problems are related with the equation

$$y = x^a \pmod n.$$

Exponentiation problem Given x, a, n, compute y
Easy: it can be done in polynomial time

Discrete logarithm problem Given x, y, n, compute a
Very hard. It is believed that the discrete logarithm problem is $\mathbf{NP}$-hard even in the average case. (A formal proof of it would imply that exponentiation is a one-way function.)

Root finding problem Given y, a, n, compute x
Hard.

Square root finding problem Given $y, a = 2, n$, compute x
This problem is in general as hard as factorization.

Square root finding can be done by a randomized polynomial time algorithm if

- n is a prime;

or

- the prime decomposition of n is know.

Groups $\mathbb{Z}_n$ and $\mathbb{Z}_n^\star$

Two integers a, b are congruent modulo n if

$$a \bmod n = b \bmod n.$$

Notation: $a \equiv b \pmod{n}$

Let $+_n, \times_n$ denote addition and multiplication modulo n

$$a +_n b = (a + b) \bmod n$$
$$a \times_n b = (ab) \bmod n$$

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a group under the operation $+_n$.

$\mathbb{Z}_n^\star = \{x | 1 \le x \le n, \gcd(x, n) = 1\}$ is a group under the operation $\times_n$

$\mathbb{Z}_n^\star$ is a field under the operations $+_n, \times_n$ if n is a prime

Theorem For any n, the multiplicative inverse of any $z \in \mathbb{Z}_n^\star$ can be computed in polynomial time.

Proof Computation can be done by the extended Euclid algorithm.

Theorem In the group $(\mathbb{Z}_n^\star, \times_n)$ the exponentiation can be performed in polynomial time.

Properties of the group $\mathbb{Z}_n^\star$

Definition (1) For any group $(G, \circ)$ and any $x \in G$

$$\mathrm{ord}(x) = \min\{k > 0 | x^k = 1\}$$

(2) The group $(G, \circ)$ is called cyclic if it contains an element g, called generator, such that $\mathrm{ord}(g) = |G|$.

Theorem If the multiplicative group $(\mathbb{Z}_n^\star, \times_n)$ is cyclic, then it is isomorphic to the additive group $(\mathbb{Z}_{\Phi(n)}, +_{\Phi(n)})$. (However, no effective way is known, given n, to create such an isomorphism!)

Theorem The mutliplicative group $(\mathbb{Z}_n^\star, \times_n)$ is cyclic iff n is either $1, 2, 4, p^k$ or $2p^k$ for some $k \in \mathbb{N}^+$ and an odd prime $p > 2$.

Theorem Let p be a prime. Given the prime factorization of $p - 1$ a generator for group $(\mathbb{Z}_p^\star, \times_p)$ can be found in polynomial time by a randomized algorithm.

Proof (1) Pick randomly $x \in \mathbb{Z}_p^\star$ and checks whether its order is $p - 1$. If yes, it is a generator. The probability to find a generator in a single trial is

$$\frac{\Phi(p-1)}{p-1} = \Omega\left(\frac{1}{p}\right).$$

How to check whether the order of x is $p - 1$? Let $p_1, \dots, p_t$ be different prime factors of $p - 1$. If $\mathrm{ord}(x) < p - 1$, then $\mathrm{ord}(x)$ has to be proper divisor of $p - 1$, that is for some p_i,

$$\mathrm{ord}(x) \left| \frac{p-1}{p_i} \right.$$

To verify that $\mathrm{ord}(x) = p - 1$, it suffices to check for each p_i, that

$$x^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}.$$

Quadratic residues and nonresidues

An integer $x \in \mathbb{Z}_m^\star$ is called a quadratic residue modulo m if

$$x \equiv y^2 (\bmod\ m)$$

for some $y \in \mathbb{Z}_m^\star$, otherwise x is a quadratic nonresidue.

Notation: QR_m – the set of all quadratic residues modulo m.
QNR_m – the set of all quadratic nonresidues modulo m.

How to decide whether an x is a quadratic residue?

Theorem If $p > 2$ is a prime and $g \in \mathbb{Z}_p^\star$ a generator, then g^k is a quadratic residue iff k is even.

Proof If k is even, then $g^{\frac{k}{2}}$ is the square root of g^k.
Let $k = 2l + 1$ and $x \in \mathbb{Z}_p^\star$ be such that $x^2 = g^{2k+1} (\bmod\ p)$.
If $x = g^m$, then $g^{2m} \equiv g^{2k+1} (\bmod\ p)$ and therefore in the additive group modulo $\Phi(p)$ it holds

$$2m = 2l + 1 (\bmod\ \Phi(p))$$

Since $\Phi(p) = p - 1$, this is impossible.

Theorem If p is a prime, then $a \in \mathbb{Z}_p^\star$ is a quadratic residue iff

$$a^{\frac{p-1}{2}} \equiv 1 (\bmod\ p).$$

Proof (1) If $a \in QR_p, a = q^{2k} (\bmod\ p)$ for some generator q,
$a^{\frac{p-1}{2}} \equiv_p q^{k(p-1)} \equiv_p (q^{p-1})^k \equiv_p 1^k \equiv 1.$
(2) If $a \in QNR_p, a = q^{2k+1} (\bmod\ p)$ for some generator q, then
$a^{\frac{p-1}{2}} \equiv_p q^{k(p-1)} q^{\frac{p-1}{2}} \equiv_p q^{\frac{p-1}{2}} \equiv_p -1.$

Euler's criterion

Theorem Let $p > 2$ be a prime. Then x is a quadratic residue modulo p if and only if

$$x^{(p-1)/2} \equiv 1 \pmod p.$$

Proof First suppose that $x \equiv y^2 \pmod p$. From Fermat theorem it follows that $x^{p-1} \equiv 1 \pmod p$ if $x \not\equiv 0 \pmod p$. Therefore

$$\begin{aligned} x^{(p-1)/2} &\equiv (y^2)^{(p-1)/2} \pmod p && (17)\\ &\equiv y^{p-1} \pmod p && (18)\\ &\equiv 1 && (19) \end{aligned}$$

Secondly, let $x^{(p-1)/2} \equiv 1 \pmod p$. Then $x \equiv b^i \pmod p$ for some primitive element modulo p and some i. Therefore

$$\begin{aligned} x^{(p-1)/2} &\equiv (b^i)^{(p-1)/2} \pmod p && (20)\\ &\equiv b^{i(p-1)/2} \pmod p && (21) \end{aligned}$$

Since b has order $p-1$, it must be the case that $p-1$ divides $i(p-1)/2$ and therefore i has to be even. Therefore the square roots of x are $\pm b^{i/2}$.

Examples

$n = 8 \quad \mathbb{Z}_8^\star = \{1, 3, 5, 7\}$

$$1^2 \equiv 1 \mod 8,\ 2^2 \equiv 4 \mod 8,\ 3^2 \equiv 1 \mod 8,\ 4^2 \equiv 0 \mod 8,$$
$$5^2 \equiv 1 \mod 8,\ 6^2 \equiv 4 \mod 8,\ 7^2 \equiv 1 \mod 8$$

$$QR_8 = \{1\}$$

$n = 9 \quad \mathbb{Z}_9^\star = \{1, 2, 4, 5, 7, 8\}$

$1^2 \equiv 1 \mod 9,\ 2^2 \equiv 4 \mod 9,\ 3^2 \equiv 0 \mod 9,\ 4^2 \equiv 7 \mod 9,$
$5^2 \equiv 7 \mod 9,\ 6^2 \equiv 0 \mod 9,\ 7^2 \equiv 4 \mod 9,\ 8^2 \equiv 1 \mod 9$

$$QR_9 = \{1, 4, 7\}$$

$n = 15 \quad \mathbb{Z}_{15}^\star = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$1^2 \equiv 1 \mod 15,\ 2^2 \equiv 4 \mod 15,\ 3^2 \equiv 9 \mod 15,\ 4^2 \equiv 1 \mod 15,$
$5^2 \equiv 10 \mod 15,\ 6^2 \equiv 6 \mod 15,\ 7^2 \equiv 4 \mod 15,\ 8^2 \equiv 4 \mod 15,$
$9^2 \equiv 6 \mod 15,\ 10^2 \equiv 10 \mod 15,\ 11^2 \equiv 1 \mod 15,\ 12^2 \equiv 9 \mod 15,$
$13^2 \equiv 4 \mod 15,\ 14^2 \equiv 1 \mod 15$

$$QR_{15} = \{1, 4\}$$

FINDING of QUADRATIC (NON)RESIDUES

Let p be a prime.

How to find (1) a quadratic residue in QR_p? ?
(2) How to find a quadratic nonresidue in QNR_p

(1) Very easy: choose a, compute a^2
(2) Very easy using a randomized algorithm because exactly half of elements are quadratic nonresidues.

If the generalized Riemann Hypothesis holds, then $\mathbb{Z}_p^\star$ has to contain a quadratic nonresidue among its $\mathcal{O}(\log^2 p)$ smallest elements.

Legendre and Legendre-Jacobi symbols

The following notation is useful to deal with quadratic residues and nonresidues:

$$(x|m)\begin{cases} 1 & \text{if } x \in QR_m \text{ and } m \text{ is prime} \\ -1 & \text{if } x \in QNR_m \text{ and } m \text{ is prime} \\ \Pi_{i=1}^{n}(x|p_i) & \text{if } m = \Pi_{i=1}^{n} p_i,\ p_i \text{ are primes, } \gcd(x,m)=1 \end{cases}$$

$(x|m)$ is called the Legendre symbol if m is prime and the Legendre-Jacobi symbol otherwise.

Rules to compute $(x|m)$

1. Euler's criterion: $x|p \equiv x^{\frac{p-1}{2}} (\text{mod } p)$ if $p > 2$ is prime, $x \in \mathbb{Z}_p^\star$
2. If $x \equiv y (\text{mod } m)$, then $(x|m) = (y|m)$.
3. $(x|m) \cdot (y|m) = (xy|m)$.
4. $(-1|m) = (-1)^{\frac{m-1}{2}}$, if m is odd.
5. $(2|m) = (-1)^{\frac{m^2-1}{8}}$, if m is odd
6. Law of quadratic reciprocity: If $\gcd(m,n) = 1, m, n$ are odd, then

$$(n|m)(m|n) = (-1)^{\frac{(m-1)(n-1)}{4}}$$

Example

$$\begin{aligned} (28|97) &= (2|97)(2|97)(7|97) = (7|97) \\ &= (97|7)(-1)^{\frac{(97-1)(7-1)}{4}} = (6|7) \\ &= (2|7)(3|7) = (-1)^6(3|7) = (7|3)(-1)^3 = -(1|3) = -1 \end{aligned}$$

Solovay-Strassen's prime recognition algorithm

It follows from the Lagrange theorem that if the following fast Monte Carlo algorithm — based on the fact that computation of Legendre-Jacobi symbols can be done fast — reports that a given number n is composite, then this is 100%, true and if it reports that it is a prime, then the error is at most $\frac{1}{2}$.

begin choose randomly an integer $a \in \{1, \ldots, n\}$
    if $\gcd(a, n) \neq 1$ then return "composite"
        else **if** $(a|n) \not\equiv a^{\frac{n-1}{2}} (\mathrm{mod}\ \ n)$
            then **return** "composite";
    return "prime"
end

Indeed, if n is composite, then all integers $a \in \mathbb{Z}_n^\star$ such that

$$(a|n) \equiv a^{\frac{n-1}{2}} (\mathrm{mod}\ \ n)$$

form a proper subgroup of the group $\mathbb{Z}_n^\star$. This implies that most of the elements $a \in \mathbb{Z}_n^\star$ are such that

$$(a|n) \not\equiv a^{\frac{n-1}{2}} (\mathrm{mod}\ \ n)$$

and therefore they can "witness" compositness of n, if n is composite.

How many square roots there exist?

Theorem
(1) If $p > 2$ is a prime, $k \geq 1$, then any quadratic residue modulo p^k has exactly two distinct square roots $x, -x = p^k - x$
(2) If $p = 2$, $k \geq 1$, then any quadratic residue modulo 2^k has
- 1 square root if $k = 1$;
- 2 square root if $k = 2$;
- 4 square root if $k > 2$.

Theorem If an odd number n has exactly t distinct factors, then any quadratic residue a modulo n has exactly 2^t distinct square roots.

We show the theorem only for the case $n = p \cdot q$ where $p > 2, q > 2$ are primes.

Let $a \in QR_n, a \equiv a_1^2 (\bmod n)$.

By the Chinese Remainder Theorem there are integers u, v such that

$$u \equiv a_1 \mod p \qquad u \equiv -a_1 \mod q$$

$$v \equiv a_1 \mod q \qquad v \equiv -a_1 \mod p$$

Since p, q are odd, u, v have to be distinct. Moreover,

$$u^2 \equiv v^2 \equiv a_1^2 \mod pq$$

and therefore $a_1, -a_1, u, v$ are 4 different square roots.

COMPUTATION of DISCRETE SQUARE ROOTS

Theorem (Adleman-Manders-Miller)
There exists a randomized polynomial time algorithm to compute the square root of modulo p, where $a \in QR_p$, and p is a prime.

Theorem There is a polynomial algorithm which computes, given x, u, v, p, q such that

$$x \equiv u^2 \mod p, x \equiv v^2 \mod q, p, q\text{-primes}$$

a w such that $x \equiv w^2 \mod pq$.
Proof Let x, u, v, p, q satisfy the above conditions.
Using Euclid's algorithm we can compute a, b such that

$$ap + bq = 1$$

If we denote

$$c = bq = 1 - ap, \quad d = ap = 1 - bq,$$

then

$$c \equiv 0 \bmod q, d \equiv 0 \bmod p, c \equiv 1 \bmod p, d \equiv 1 \bmod q.$$

We show now that for $w = cu + dv$ we have

$$x \equiv w^2 \bmod p, x \equiv w^2 \bmod q$$

and therefore

$$x \in QR_p, x \in QR_q \Rightarrow x \in QR_{pq}.$$

Case 1. $w^2 = (cu + dv)^2 = c^2u^2 + 2cduv + d^2v^2 \equiv u^2 \equiv x (\mod p)$
Case 2. $w^2 = (cu + dv)^2 = c^2u^2 + 2cduv + d^2v^2 \equiv v^2 \equiv x (\mod q)$

Blum's integers

Blum's integers have the form

$$n = p \cdot q, \quad p, q \text{ are primes}, \quad p \equiv q \equiv 3 (\bmod\ 4).$$

Why are Blum integers of importance?

Theorem If n is a Blum integer, then the mapping

$$x \to x^2 \bmod n$$

is a permutation on QR_n.

(In other words, in such a case each quadratic residue has a unique square root that is also a quadratic residue and it is called its principal square root.)

RABIN'S ALGORITHM

Theorem (Rabin) The following statements are equivalent:
(1) There is a polynomial time randomized algorithm to factor Blum integers.
(2) There is a polynomial time randomized algorithm to compute the principal square root for $x \in QR_n$, if n is a Blum integer.

Proof (1) Assume, that a polynomial time randomized algorithm $\mathcal{A}$ to compute the principal square root modulo Blum integers is given.
A Blum integer n can be factorized as follows:

1. Choose randomly a y such that $(y|n) = -1$.
2. Compute $x \equiv y^2 \mod n$.
3. Find, using $\mathcal{A}$, a $z \in QR_n$ such that $x = z^2 \mod n$.

We show that $\gcd(y+z, n)$ is a prime factor of $n = pq$.
Clearly pq divides $(y-z)(y+z)$. Since

$$(-z|n) = (-1|n)(z|n) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}}(z|n) =??$$

we have $y \not\equiv -z \mod n$ and therefore $\gcd(y+z, n)$ has to be one of the prime factor of n.
(2) Assume we can effeciently factor $n = pq$.
We show how to compute effeciently principal square roots modulo n.
Let $x \in QR_n$. Using Adleman-Manders-Miller's algorithm compute

$$u \in QR_p, v \in QR_q \text{ such that } x = u^2 \bmod p, y = v^2 \bmod q.$$

Using extended Euclid's algorithm compute a, b such that $ap + bq = 1$.
Compute $c = bq, d = ap$.
We show that $w = cu + dv \in QR_n$ and it is a square root of x. Since

$$c \equiv 1 \mod p, d \equiv 1 \bmod q$$

and

$$w^2 \equiv u^2 \equiv x \mod p, w^2 \equiv v^2 \equiv x \mod q$$

we have

$$w^2 \equiv x \mod n.$$

To show $w \in QR_n : (w|pq) = (w|p)(w|q) = (u|p)(v|q) = 1$.