Part I

Appendix

APPENDIX to IO54

NOTATION

- Logarithms.
  - $\log_b a$ - logarithm of a at the base b.
  - $\log n$ - logarithm at the base 10 - decimal logarithm.
  - $\lg n$ - logarithm at the base 2 - binary logarithm
  - $\ln n$ - logarithm at the base e - natural logarithm
- For complexity of algorithms depending on an integer n the following shorthand is often used:

$$L_n(\alpha, c) = e^{(c+o(1))(\ln n)^{\alpha}(\ln \ln n)^{1-\alpha}}$$

with $0 \leq \alpha \leq 1$ and $c > o$. The parameter α is the more important one. Deepending on it, $L_n(\alpha, c)$ interpolates between polynomial complexity for $\alpha = 0$ and exponential complexity for $\alpha = 1$. For $\alpha < 1$ the complexity is said to be subexponential.

TWO CENTRAL CONCEPTS of MODERN CRYPTOGRAPHY

- **Efficient computation** is usually modelled by computations that are polynomial-time in an input (security) parammeter
- **Efficient (computational) indistinguishability**. We say that probability ensembles $X = \{X_\alpha\}_{\alpha \in S}$ and $Y = \{Y_\alpha\}_{\alpha \in S}$ are computationally indistinguishable if for every family of polynomial-size circuits $\{D_n\}$, every polynomial p, all sufficiently large n and every $\alpha \in \{0,1\}^n \cap S$,

$$|Pr[D_n(X_\alpha) = 1] - Pr[D_n(Y_\alpha) = 1]| < \frac{1}{p(n)}$$

where the probabilities are taken over the relevant distribution (i.e., either X_n or Y_n).

BASICS of ABSTRACT ALGEBRAS

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 element e such 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 $a * a^{-1} = a^{-1} * a = e$.

A group G is called **Abelian group** 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?

Groups Z_n and Z_n^*

Two integers a, b are congruent modulo n if

$$a \mod n = b \mod n.$$

Notation: $a \equiv b (\mod n)$
Let $+_n, \times_n$ denote addition and multiplication modulo n

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

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

$\mathbf{Z_n^\star} = \{x | 1 \leq x \leq n, \gcd(x, n) = 1\}$ is a group under the operation $\times_n$

$\mathbf{Z_n^\star}$ is a field under the operations $+_n, \times_n$ if n is a prime
Theorem For any n, the multiplicative inverse of any $m \in \mathbf{Z_n^\star}$ can be computed in polynomial time.
Comment: Computation can be done by the extended Euclid algorithm.
Theorem In the group $(\mathbf{Z_n^\star}, \times_n)$ the exponentiation can be performed in polynomial time.

- If a is an element of a finite group G, then its **order** is the smallest integers k such that $a^k = 1$.
- Order of each element of a group G is a divisor of the number of elements of G.
- This implies that every element $a \in \mathbf{Z}_p^*$, where p is a prime, has order $p-1$ and it holds

$$a^{p-1} \equiv 1 \ (\mathrm{mod}) p$$

PROPERTIES of the GROUP $\mathbf{Z_n^\star}$

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

$$\text{order of } x = \min\{k > 0 | x^k = 1\}$$

(2) The group $(G, \circ)$ is called cyclic if it contains an element g, called generator, such that the order of $(g) = |G|$.

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

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

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

Proof (1) Pick randomly $x \in Z_p^\star$ 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 $p_1, \ldots, p_t$ be different prime factors of $p - 1$. If order of $x < p - 1$, then the order of x has to be proper divisor of $p - 1$, that is for some p_i,

$$\text{order of} x \left| \frac{p-1}{p_i} \right.$$

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 laws hold $(a \cdot (b + c) = a \cdot b + a \cdot c$ a $(b + c) \cdot a = b \cdot a + c \cdot a)$ a for all $a, b, c \in R$.

A ring is called **commutative ring** 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 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.

FINITE FIELDS GF(p^n)

There are two important ways GF(4), the Galois field of four elements, is realized.
1. It is easy to verify that such a field is the set

$$\mathrm{GF}(4) = \{0, 1, \omega, \omega^2\}$$

with operations $+$ and $\cdot$ satisfying laws

- $0 + x = x$ for all x;
- $x + x = 0$ for all x;
- $1 \cdot x = x$ for all x;
- $\omega + 1 = \omega^2$

2. Let $\mathbf{Z}_2[x]$ be the set of polynomials whose coefficients are integers mod 2. GF(4) is also $\mathbf{Z}_2[x] \pmod{x^2 + x + 1}$ therefore the set of polynomials

$$0, 1, x, x + 1$$

where addition and multiplication are $\pmod{x^2 + x + 1}$.

3. Let p be a prime and $\mathbf{Z}_p[x]$ be the set of polynomials with coefficients mod p. If $p(x)$ is a irreducible polynomial $\bmod p$ of degree n, then $\mathbf{Z}_p[x] \pmod{p(x)}$ is a GF(p^n) with p^n elements.

BASICS of NUMBER THEORY

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.

CEILING and FLOOR FUNCTIONS

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

Example

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

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

MODULO OPERATIONS

The remainder of n when 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

$$7 \mod 5 = 2 \qquad 122 \mod 11 = 1$$

Identities

- $(a+b) \mod n = ((a \mod n) + (b \mod n)) \mod n$
- $(a \cdot b) \mod n = ((a \mod n) \cdot (b \mod n)) \mod n$
- $a^b \mod n = ((a \mod n)^b) \mod n.$

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

EUCLID ALGORITHM for GCD - I.

This is algorithm to compute greatest common divisor (gcd) of two integers, in short

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

EUCLID ALGORITHM

$$\begin{aligned} \text{gcd}(0, n) &= n & (1) \\ \text{gcd}(m, n) &= \text{gcd}(n \mod m, m) \text{ for } m > 0 & (2) \end{aligned}$$

Example

$$gcd(296, 555) = gcd(259, 296) = gcd(37, 259) = gcd(0, 37) = 37$$

because

$$555 = 1 \times 296 + 259$$
$$296 = 1 \times 259 + 37$$
$$259 = 7 \times 37 + 0$$

EUCLID ALGORITHM for GCD - II.

Theorem $T(n) = \mathcal{O}(\log n)$ for the number of steps of Euclid's algoritm.
Example 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.
Problem: Is there an asymptotycally faster algorithm to compute gcd(m, n)?

EXTENDED EUCLID 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.
Example: 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: $a^n \mod m = ((a \mod m)^n) \mod m$
Modular multiplication: $ab \mod n = ((a \mod n)(b \mod n) \mod n)$
Example $3^{1000} \mod 19 = 16$
$3^{10000} \mod 13 = 3$
$3^{340} \mod 11 = 1$
$3^{100} \mod 79 = 51$

PRIMES

Primes play key role in modern cryptography.

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 a prime?

- Only in 2002 it has been shown that there is a $(O(m^{12}))$ deterministic algorithm to recognize whether an m bit integer is a prime.
- There are (very) simple randomized algorithm to decide fast and with large

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

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

and the solution $(\star)$ is unique up to the congruence modulo M.
Each integer $0 < x < M$ is uniquelly represented by t-tuple: $x \pmod{m_1}, \ldots, x \pmod{m_t}$.
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

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

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.

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

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

(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

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

EULER and FERMAT 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 $a < p$, $a^{x-y} = a^{k(p-1)} \equiv 1 \mod p$

- **Carmichel numbers** They are composite integers n that satisfy the the congruence

$$b^n \equiv b(\mod n)$$

for all $1 < b < n$.

They are also called Fermat's pseudoprimes, because they are not primes, but they pass fermat primality test.

The first 7 Carmichel numbers $561, 1105, 1729, 2465, 2821, 6601, 8911$ were discoved by a Czech mathematician in 1985.

There are 20, 138. 200 Carmichel numbers between firs 10^{21} integers

DISCRETE LOGARITHMS and SQUARE ROOTS

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, even its modular version
Discrete logarithm problem Given x, y, n, compute a
Very hard. It is believed that the discrete logarithm problem is **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.

Examples
$\{x \mid \sqrt{x} \ (\textbf{mod}\ 15) = 1\} = \{1, 4, 11, 14\}$
$\{x \mid \sqrt{x} \ (\textbf{mod}\ 15) = 2\} = \emptyset$
$\{x \mid \sqrt{x} \ (\textbf{mod}\ 15) = 3\} = \emptyset$

QUADRATIC RESIDUES and NONRESIDUES

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

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

for some $y \in \mathbf{Z}_m^\star$, otherwise x is a quadratic nonresidue.
Notation: QR_m – the set of all quadratic residues modulo m. QR_m is therefore subgroup of squares in Z_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 $g \in \mathbf{Z}_p^\star$ a generator, then g^k is a quadratic residue iff k is even.
If k is even, then $g^{\frac{k}{2}}$ is the square root of g^k.
Let $k = 2l + 1$ and $x \in \mathbf{Z}_p^\star$ be such that $x^2 = g^{2k+1} (\mod p)$.
If $x = g^m$, then $g^{2m} \equiv g^{2k+1} (\mod p)$ and therefore in the additive group modulo $\Phi(p)$ it holds

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

Since $\Phi(p) = p - 1$, this is impossible.
Theorem If p is a prime, then $a \in \mathbf{Z}_p^\star$ is a quadratic residue iff

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

(1) If $a \in QR_p$, $a = q^{2k} (\mod p)$ 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 $a \in QNR_p$, $a = q^{2k+1} (\mod p)$ for some generator q, then

QUADRATIC RESIDUA and NONRESIDUA I

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

$$a +_n b = (a+b) \mod n, \qquad a \times_n b = (ab) \mod n$$

$Z_n = \{0, 1, \ldots, n-1\}$ is a group under the operation $+_n$
$Z_n^\star = \{x | 1 \leq x \leq n, \gcd(x, n) = 1\}$ is a group under the operation $\times_n$

$Z_n^\star$ is a field under the operations $+_n, \times_n$ if n is a prime. **Theorem** For any n, the

multiplicative inverse of any $z \in Z_n^\star$ and exponentiation in $Z_n^\star$ can be computed in polynomial time.
Definition An integer $x \in Z_n^\star$ is called a quadratic residue modulo n if

$$x \equiv y^2 (\mod n)$$

for some $y \in Z_n^\star$, otherwise x is a **quadratic nonresidue**.
Notation: QR(m) – the set of all quadratic residues modulo n. $QR(n)$ is therefore subgroup of squares in $\mathbf{Z}_n^\star$.
QNR(n) – the set of all quadratic nonresidues modulo n.
For any prime p the set QR(p) has $\frac{p-1}{2}$ elements.
So called Euler criterion says that if c is a quadratic residue modulo p, then $c^{(p-1)/2} \equiv 1 \pmod p$,

If $n = 8$ **then** $Z_8^\star = \{1,3,5,7\}$

$1^2 \equiv 1 (\mod 8)$, $3^2 \equiv 1 (\mod 8)$,
$5^2 \equiv 1 (\mod 8)$, $7^2 \equiv 1 (\mod 8)$

$$QR(8) = \{1\}$$

If $n = 9$ **then** $Z_9^\star = \{1,2,4,5,7,8\}$

$1^2 \equiv 1 (\mod 9)$, $2^2 \equiv 4 (\mod 9)$, $4^2 \equiv 7 (\mod 9)$,
$5^2 \equiv 7 (\mod 9)$, $7^2 \equiv 4 (\mod 9)$, $8^2 \equiv 1 (\mod 9)$

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

$1^2 \equiv 1 (\mod 15)$, $2^2 \equiv 4 (\mod 15)$, $4^2 \equiv 1 (\mod 15)$,
$7^2 \equiv 4 (\mod 15)$, $8^2 \equiv 4 \mod 15$,
$11^2 \equiv 1 (\mod 15)$, $13^2 \equiv 4 (\mod 15)$, $14^2 \equiv 1 (\mod 15)$

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

QUADRATIC RESIDUES and NONRESIDUES II

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

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

for some $y \in \mathbf{Z}_\mathbf{m}^\star$, otherwise x is a quadratic nonresidue.

Notation: QR_m – the set of all quadratic residues modulo m. QR_m is therefore subgroup of squares in Z_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 $g \in Z_p^\star$ a generator, then g^k is a quadratic residue iff k is even.

If k is even, then $g^{\frac{k}{2}}$ is the square root of g^k.

Let $k = 2l + 1$ and $x \in Z_p^\star$ be such that $x^2 = g^{2k+1} (\mod p)$.

If $x = g^m$, then $g^{2m} \equiv g^{2k+1} (\mod p)$ and therefore in the additive group modulo $\Phi(p)$ it holds

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

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

Theorem If p is a prime, then $a \in Z_p^\star$ is a quadratic residue iff

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

(1) If $a \in QR(p), a = q^{2k} (\mod p)$ 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 $a \in QNR(p), a = q^{2k+1} (\mod p)$ for some generator q, then

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_n?
(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 $\mathbf{Z}_\mathbf{p}^\star$ has to contain a quadratic nonresidue among its $O(\log^2 p)$ the smallest elements.

BLUM INTEGERS

If p, q are primes such that $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$ then the integer $n = pq$ is called **Blum integer**

Blum integers n have the following important properties.

- If $x \in QR(n)$, then x has exactly four square roots and exactly one of them is in QR(n) – this square root is called **primitive square root** of x modulo n.
- Function $f : QR(n) \to QR(n)$ defined by $f(x) = x^2$ is a permutation on $QR(n)$.
- The inverse function is $f^{-1}(x) = x^{((p-1)(q-1)+4)/8} \mod n$

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.
(1) Assume, that a polynomial time randomized algorithm 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 $\mathcal{A}, z \in QR_n$ 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

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

Using extended Euclid's algorithm compute a, b such that $ap + bq = 1$.

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

$$\begin{aligned} x^{(p-1)/2} &\equiv (y^2)^{(p-1)/2} \pmod p &(3)\\ &\equiv y^{p-1} \pmod p &(4)\\ &\equiv 1 &(5)\end{aligned}$$

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

$$\begin{aligned} x^{(p-1)/2} &\equiv (b^i)^{(p-1)/2} \pmod p &(6)\\ &\equiv b^{i(p-1)/2} \pmod p &(7)\end{aligned}$$

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 $\pm b^{i/2}$.

The following notation is useful to deal with quadratic residues and nonresidues: $(x|m) = \begin{cases} 1 & \text{if} x \in QR_m \text{and} m \text{is prime} \\ -1 & \text{if } x \in QNR_m \text{and} m \text{is prime} \\ \prod_{i=1}^{n}(x|p_i) & \text{if} m = \prod_{i=1}^{n} p_i, p_i \text{are primes}, \gcd(x, m) = 1 \end{cases}$

$(x|m)$ is called the Legendre symbol if m is prime and the Legendre-Jacobi (or Jacobi) symbol otherwise. There are efficient algorithms to compute Jacobi symbols.

Some useful rules to compute $(x|m)$

1. Euler's criterion: $x|p \equiv x^{\frac{p-1}{2}} \pmod{p}$ if $p > 2$ is prime, $x \in \mathbf{Z}_\mathbf{p}^\star$
2. If $x \equiv y \pmod{m}$, 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 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 $a \in \{1, \dots, n\}$
    if $\gcd(a, n) \neq 1$ then return "composite"
        else if $(a|n) \not\equiv a^{\frac{n-1}{2}} \pmod{n}$
            then return "composite";
    return "prime"
end

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

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

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

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

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

HOW MANY SQUARE ROOTS 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 $a \in QR_n, a \equiv a_1^2 (\mod n)$.
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 n 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 $x \equiv w^2 \mod pq$.
Example 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

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

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

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

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.