Modular arithmetic

Definitions

Operations happen in the set of integers, $\mathbb{Z}$. The usual addition ($+$) and multiplation ($.$ or $\times$) are well defined in this set (for more details, cf. Peano axioms).

Theorem 1 (Euclidean division)

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}^*, \exists !(q,r) \in \mathbb{Z}^2, \begin{cases} 0 \leq r < |b| \\ a = bq + r \end{cases} \tag{1}$$

q is the quotient of the division of a by b and r the remainder.

This allows defining the modulo operation as the remainder of the Euclidean division of two integers:

$$a \mod b := r \tag{2}$$

For any $b \in \mathbb{Z}^*$, it is therefore possible to define the modulo relationship, $\mathcal{R}_b$:

$$\forall (x,y) \in \mathbb{Z}^2, x \mathcal{R}_b y \iff (x-y) \mod b = 0 \tag{3}$$

This binary relation is an equivalence relation, as it is:

- reflexive ($x \mathcal{R}_b x$),
- symmetric ($x \mathcal{R}_b y \iff y \mathcal{R}_b x$),
- transitive ($x \mathcal{R}_b y \wedge y \mathcal{R}_b z \Rightarrow x \mathcal{R}_b z$).

This relation is usually written using a congruence syntax:

$$x \mathcal{R}_b y \iff x \equiv y [b] \tag{4}$$

Like any equivalence relation, $\mathcal{R}_b$ has equivalence classes. Each equivalence class holds a unique integer $r \in [\![0, |b|[\![$ (because of the Euclidean division theorem). This integer is the canonical representative of its class.

The equivalence class which contains 0 is written $\bar{0}$:

$$\forall x \in \mathbb{Z}, x \in \bar{0} \iff x \mod b = 0 \tag{5}$$

So this is the set of the multiples of b. This set is usually written $b\mathbb{Z}$.

In algebra, the set of the equivalence classes of a relation is written as a division $(\mathbb{Z}/\mathcal{R}_b)$. When the function which maps items to their equivalence class is a morphism, this set can also be written using the kernel of the morphism (i.e. the items which maps to the neutral element of the set of equivalent classes). Here, the addition maps naturally to the set of equivalence classes, and the said kernel is $b\mathbb{Z}$. This is why $\mathbb{Z}/\mathcal{R}_b$ is often written as $\mathbb{Z}/b\mathbb{Z}$.

Greatest common divisor

Definition 1 (Greatest common divisor) *The greatest common divisor between two integers a and b which are not both zero is the greatest positive integer which divides both a and b. It is written* $\gcd(a, b)$.

Theorem 2 (Bézout's identity) *For two integers a and b which are not both zero,*

$$\exists x, y \in \mathbb{Z}, ax + by = \gcd(a, b)$$

The extended Euclidean algorithm is an algorithm which produces such x and y.

Theorem 3 (Euclid's lemma) *If p is a prime number and a and b two integers,*

$$p|ab \Leftrightarrow p|a \vee p|b$$

Theorem 4 (Generalization of Euclid's lemma) *If n, a and b are integers,*

$$\gcd(n, a) = 1 \wedge n|ab \Rightarrow n|b$$

Chinese remainder theorem

Theorem 5 (Chinese remainder theorem) *Let $(n_1, n_2..., n_k) \in \mathbb{N}^{*k}$ be k pairwise coprime numbers (i.e. $i \neq j \Rightarrow \gcd(n_i, n_j) = 1$) and N the product of these numbers. Let $(\bar{a_1}..., \bar{a_k}) \in \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}$. There is only one $x \in [\![0, N-1]\!]$ such that:*

$$\forall i \in [\![1, k]\!], x \equiv a_i[n_i] \tag{6}$$

Proof of uniqueness: if x and y verify the equation, $(x - y)$ is a multiple of every n_i. As these numbers are pairwise coprime, $(x - y)$ is a multiple of their product, N, so $x = y$.

Proof of existence:

As n_1 and n_2 are coprime, Bézout's identity (and the Extended Euclidean algorithm) gives two integers u_1 and u_2 such that:

$$u_1 n_1 + u_2 n_2 = 1 \tag{7}$$

Let $x_{12} = a_1 u_2 n_2 + a_2 u_1 n_1$.

$$x_{12} = a_1(1 - u_1 n_1) + a_2 u_1 n_1 \equiv a_1[n_1] \tag{8}$$
$$x_{12} = a_1 u_2 n_2 + a_2(1 - u_2 n_2) \equiv a_2[n_2] \tag{9}$$

If $k = 2$, this ends the proof. Otherwise, it is possible to replace (n_1, a_1) and (n_2, a_2) with $(n_1 n_2, x_{12})$, decrease k by 1 and iterate until k equals 2.

Theorem 6 (Mapping of the Chinese remainder theorem) *Let $(n_1, n_2..., n_k) \in \mathbb{N}^{*k}$ be k pairwise coprime numbers and N the product of these numbers. The following function exists and is an isomorphism for the addition and the multiplication:*

$$\begin{array}{rcl} \mathbb{Z}/N\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z} \\ \bar{x} & \mapsto & \left(\overline{x \mod n_1}, \overline{x \mod n_2}..., \overline{x \mod n_k}\right) \end{array} \tag{10}$$

Modular inverse

Let $n \in \mathbb{N}$. $x \in \mathbb{Z}/n\mathbb{Z}$ is invertible if there exists $y \in \mathbb{Z}/n\mathbb{Z}$ such that $xy = \bar{1}$. As the multiplication is commutative, this implies that $yx = \bar{1}$ too. The set of invertible items of $\mathbb{Z}/n\mathbb{Z}$ is written $(\mathbb{Z}/n\mathbb{Z})^\times$.

This y is unique. Indeed, if there exists y_1 and y_2 with this property,

$$y_1 = y_1.1 = y_1 x y_2 = 1.y_2 = y_2 \tag{11}$$

This y is called the inverse of x and is written x^{-1}.

When talking about integers instead of equivalence classes, the definitions become:

- $x \in \mathbb{Z}$ is invertible modulo n if there exists $y \in \mathbb{Z}$ such that $xy \equiv 1[n]$.
- The inverse of such x modulo n is the integer $y \in [\![0, n[\![$ such that $xy \equiv 1[n]$.
- The set of integers invertible modulo n is also written $(\mathbb{Z}/n\mathbb{Z})^\times$, in a kind of language abuse.

When $x \in \mathbb{Z}$ is invertible modulo n:

$$\exists (y, q) \in \mathbb{Z}^2, xy = qn + 1 \tag{12}$$
$$\exists (u, v) \in \mathbb{Z}^2, ux + vn = 1 \tag{13}$$

This last equation can be used to show that there is no common divisor except 1 between x and n (this is Bézout's identity). Moreover, for any $x \in \mathbb{Z}$ the Extended Euclidean algorithm builds two integers u and v such that:

$$ux + vn = \gcd(x, n) \tag{14}$$

If x and n share no divisor except 1, their greatest common divisor is 1, which leads to:

$$ux + vn = 1 \tag{15}$$
$$ux \equiv 1[n] \tag{16}$$

This gives a way to compute the inverse of x modulo n, and leads to the following theorem.

Theorem 7 (Modular inverse)

$$\forall n \in \mathbb{N}, \forall x \in \mathbb{Z}, x \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \gcd(x, n) = 1 \tag{17}$$

Euler totient function

Definition 2 (Euler totient function) *For $n \in \mathbb{N}^*$, the Euler totient function of n, $\phi(n)$, is the number of integers in $[\![1, n[\![$ which are relatively prime to n:*

$$\begin{array}{rccl} \phi : \mathbb{N}^* & \to & \mathbb{N}^* \\ n & \mapsto & |\{x \in [\![1, n[\![, \gcd(x, n) = 1\}| \end{array} \tag{18}$$

Using theorem 7, it is straightforward to link this function with the set of inverses modulo n.

Theorem 8 (Alternative definition of Euler totient function)

$$\forall n \in \mathbb{N}^*, \phi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| \tag{19}$$

Here are some properties of this function:

$$\phi(1) = 1 \tag{20}$$

If p is a prime number, every integer between 1 and $p - 1$ is relatively prime to p, so:

$$\forall p \in \mathbb{P}, \phi(p) = p - 1 \tag{21}$$

Moreover for $k \geq 2$, if $x \in \mathbb{N}^*$ is not relatively prime to p^k, $\gcd(x, p^k) \neq 1$ and a divisor of p^k divides x. As every divisor of p^k is a multiple of p, x is also a

multiple. Reciprocally every multiple of p cannot be relatively prime to p^k. So the number of integers between 1 and $p^k - 1$ which are relatively prime to p^k is:

$$\forall p \in \mathbb{P}, \forall k \in \mathbb{N}^*, \phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right) \tag{22}$$

If m and n are relatively primes one to each other, the Chinese remainder theorem (theorem 6) helps defining an isomorphism between $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}\times \mathbb{Z}/n\mathbb{Z}$ relativelity to the multiplication. This morphism can be restricted to an isomorphism between $(\mathbb{Z}/mn\mathbb{Z})^\times$ and $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. The existence of this isomorphism leads to the following proposition:

$$\forall m, n \in {\mathbb{N}^*}^2, \gcd(m,n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n) \tag{23}$$

Galois fields over prime numbers

When a set is provided with addition and multiplication operations, like $(\mathbb{Z}/n\mathbb{Z}, +, .)$, it is called a field when every non-zero item is invertible.

If n is a prime number, no integer between 1 and $n-1$ shares any divisor except 1 with n, so every equivalence class of $\mathbb{Z}/n\mathbb{Z}$ which is not $\bar{0} = n\mathbb{Z}$ is invertible.

Otherwise (if n is not a prime number), there exists $d \in [\![2, n-1]\!]$ which divides n, and this d is therefore not invertible modulo n.

Theorem 9 (Finite fields $\mathbb{Z}/n\mathbb{Z}$) *For $n \in \mathbb{N}$, $(\mathbb{Z}/n\mathbb{Z}, +, .)$ is a finite field if and only if n is a prime number.*

Évariste Galois is a famous mathematician who gave his name to the finite fields, which are fields with a finite number of items (contrary to infinite fields like the set of real numbers). He showed that the finite fields with a prime number of items can be mapped to $\mathbb{Z}/n\mathbb{Z}$, with n being this number of items.

As a prime number is usually written $p \in \mathbb{P}$, this leads to using $\mathbb{Z}/p\mathbb{Z}$ to speak of the finite field with p items. This field can also be written $\mathbb{F}_p$ or $\mathrm{GF}(p)$ in the literature.

Fermat's little theorem

Theorem 10 (Fermat's little theorem) *With p a prime number,*

$$\forall a \in \mathbb{Z}, a^p \equiv a[p] \tag{24}$$

There exist several proofs of this theorem[1]. Let's write down here a proof using modular arithmetic.

[1] https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem

Proof of Fermat's little theorem using modular arithmetic

First, let's reduce the set of a to the positive integers between 1 and $p-1$.

- If p is odd, $(-1)^p = -1$ so $(-1)^p \equiv -1[p]$. Otherwise p is an even prime number, so $p = 2$ and $(-1)^p = 1 \equiv -1[2]$. The theorem is therefore true for $a = -1$.
- If Fermat's little theorem is true for $a \in \mathbb{N}$, it is true of negative integers as well, because $(-a)^p = (-1)^p a^p \equiv -1.a = -a[p]$
- If Fermat's little theorem is true for $a \in [\![0, p-1]\!]$, it can be extended for $a \in \mathbb{N}$ because every operation is modulo p.
- The theorem is trivially true for $a = 0$, because $a^p = 0$ (p cannot be null).

Therefore if the theorem is true for $a \in [\![1, p-1]\!]$, it will be true for $a \in \mathbb{Z}$.

With $a \in [\![1, p-1]\!]$, let's study the sequence $(a, 2a, 3a...(p-1)a)$ modulo p:

$$\forall i \in \mathbb{N}, u_i := ia \mod p \tag{25}$$

As a is invertible modulo p,

$$\forall i \in \mathbb{N}, u_i = 0 \iff ia = 0 \mod p \iff i = 0 \mod p \tag{26}$$

$$\forall i \in [\![1, p-1]\!], u_i \neq 0 \tag{27}$$

Moreover, for $(i, j) \in \mathbb{N}^2$ such that $1 \leq i < j \leq p-1$,

$$u_j - u_i = ja - ia = (j-i)a \equiv u_{j-i}[p] \tag{28}$$

If $u_j = u_i$, $u_{j-i} \equiv 0[p]$ so $u_{j-i} = 0$ because $u_{j-i} \in [\![0, p[\![$. This is incompatible with $1 \leq j - i \leq p-1$.

Therefore $u_j \neq u_i$.

This shows that every item in the sequence $(u_1, u_2..., u_{p-1})$ is unique and in $[\![1, p-1]\!]$. So the products of all the items of the sequence is equals to the product of all integers between 1 and $p-1$:

$$\prod_{i=1}^{p-1} u_i = \prod_{i=1}^{p-1} i \tag{29}$$

$$\prod_{i=1}^{p-1}((ia) \mod p) = \prod_{i=1}^{p-1} i \tag{30}$$

$$\prod_{i=1}^{p-1}((ia) \mod p) \equiv \prod_{i=1}^{p-1} i[p] \tag{31}$$

$$\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} a\right) \equiv \prod_{i=1}^{p-1} i[p] \tag{32}$$

As every integer from 1 to $p-1$ is invertible,

$$a^{p-1} \equiv 1[p] \tag{33}$$

$$a^{p} \equiv a[p] \tag{34}$$

Modular inverse consequence of Fermat's little theorem

For $p \in \mathbb{P}$, and $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}$. As $a.a^{p-2} = a^{p-1} \equiv 1[p]$, the inverse of a modulo p is $a^{p-2} \mod p$.

Euler's theorem

Euler's theorem is a generalisation of Fermat's little theorem.

Theorem 11 (Euler's theorem)

$$\forall n \in \mathbb{N}^*, \forall a \in \mathbb{Z}, \gcd(a,n) = 1 \Rightarrow a^{\phi(n)} \equiv 1[n] \tag{35}$$

This theorem can be proven using Lagrange theorem on the group $((\mathbb{Z}/n\mathbb{Z})^{\times}, \times)$.

Lagrange theorem

Theorem 12 (Lagrange theorem) *For any finite group G, the number of elements (i.e. the order) of every subgroup H of G divides the number of elements of G.*

Proof of Lagrange theorem:

Let H be a subgroup of G. Let $\mathcal{R}_H$ be the relation defined by:

$$\forall (x,y) \in G^2, x\mathcal{R}_H y \iff \exists h \in H, x = yh \tag{36}$$
$$\iff y^{-1}x \in H \tag{37}$$

This defines an equivalence relation and its equivalence classes are the "cosets" of H. With $a \in G$,

$$\forall x \in G, x \in \bar{a} \iff x\mathcal{R}_H a \tag{38}$$
$$\iff \exists h \in H, x = ah \tag{39}$$
$$\iff x \in aH \tag{40}$$

Hence the equivalence class of $a \in G$ is aH.

With $(a,b) \in G^2$, the function $x \mapsto ba^{-1}x$ maps any element from aH to bH, and $x \mapsto ab^{-1}x$ is its reciproqual. This is therefore a bijection between two finite sets (because G is finite), so all equivalence classes share the same number of elements ($|aH| = |bH|$). The equivalence classes form a partition of G. With $[G:H]$ being the number of equivalence classes, this partition leads to:

$$|G| = [G:H]|H| \tag{41}$$
$$|H| \text{ divides } |G| \tag{42}$$

QED.

Proof of Euler's theorem

In order to prove Euler's theorem, let's apply it to $G = (\mathbb{Z}/n\mathbb{Z})^\times$ and $H = a^i, i \in \mathbb{N}$ with $a \in \mathbb{Z}$ such that $\gcd(a,n) = 1$. $(H, \times)$ is a subgroup of G (H is the orbit of a) and is finite. Therefore there exists $(i,j) \in \mathbb{N}^2$ such that $i < j$ and $a^i \equiv a^j[n]$. As a is invertible modulo n, $a^{j-i} \equiv 1[n]$, with $j - i > 0$. This allows to define the order of a in $(\mathbb{Z}/n\mathbb{Z})^\times$:

$$\text{ord}_n(a) := \min\left(i \in \mathbb{N}^*, a^i \equiv 1[n]\right) \tag{43}$$

Every number from $(1, a, a^2, a^3..., a^{\text{ord}_n(a)-1})$ is different modulo n, because if $a^i \equiv a^j[n]$ with $0 \leq i < j < \text{ord}_n(a)$, $a^{j-i} \equiv 1[n]$ with $j - i < \text{ord}_n(a)$. Moreover $H = \{1, a, a^2, a^3..., a^{\text{ord}_n(a)-1}\}$ because it *loops* at the order of a. Therefore:

$$|H| = \text{ord}_n(a) \tag{44}$$
$$\text{ord}_n(a) \text{ divides } |G| = |(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n) \tag{45}$$

Let $m \in \mathbb{Z}$ such that $\phi(n) = m.\text{ord}_n(a)$.

$$a^{\phi(n)} = a^{m.\text{ord}_n(a)} = \left(a^{\text{ord}_n(a)}\right)^m \equiv 1^m = 1[n] \tag{46}$$

QED.

Modular square root

The question of finding a square root r of an integer x modulo n (i.e. such that $r^2 \equiv x[n]$) has a different answer than when working on real numbers. In modular arithmetic, some numbers to not have a square root, -1 may have one, etc. and the algorithm to compute one is very different from the approximation used for real numbers.

The values $n = 1$ and $n = 2$ are not very interesting:

- $\mathbb{Z}/1\mathbb{Z}$ contains a single element, 0, which is its own square root.
- $\mathbb{Z}/2\mathbb{Z}$ contains two elements (0 and 1), which squares are themselves. So their square roots are themselves too.

Things become more interesting with $n \geq 3$.

Euler's criterion

A number is a quadratic residue if it is the square of an integer.

Theorem 13 (Euler's criterion) *With p an odd prime number and $a \in \mathbb{Z}$ coprime to p (i.e. $a \mod p \neq 0$),*

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1[p] & \text{if } a \text{ is a quadratic residue modulo } p \\ -1[p] & \text{if } a \text{ is not a quadratic residue modulo } p \end{cases} \tag{47}$$

Here is a proof.

First, according to Fermat's little theorem,

$$a^{p-1} \equiv 1[p] \tag{48}$$

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1[p] \tag{49}$$

Therefore $a^{\frac{p-1}{2}}$ is a root of $X^2 - 1 = (X-1)(X+1)$ in the finitie field $\mathbb{F}_p$, which leads to $a^{\frac{p-1}{2}} \equiv \pm 1[p]$. (This comes from the fact that $xy = 0 \Rightarrow x = 0 \vee y = 0$ in a field because every non-null element is invertible.)

By grouping the numbers in $[\![1, p-1]\!]$ by pairs $(x, p-x)$ with x being odd, each pair matches a unique quadratic residue (because $(p-x)^2 \equiv x^2[p]$) and every matched residue is distinct (because $X^2 - x^2$ has at most two roots). Therefore there are at least $\frac{p-1}{2}$ quadratic residues.

If a is a quadratic residue modulo p, let x be a square root of a. Then $x \mod p$ cannot be zero so Fermat's little theorem and the fact that p is odd give:

$$1 \equiv x^{p-1} \equiv x^{2\frac{p-1}{2}} = \left(x^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}}[p] \tag{50}$$

Therefore the polynomial $X^{\frac{p-1}{2}}-1$ has at least $\frac{p-1}{2}$ roots (the quadratic residues). As it cannot have more roots (according to Lagrange theorem on polynomials), the quadratic nonresidues are not root of this polynomial. If a is not a quadratic-residue, $a^{\frac{p-1}{2}} \equiv \pm 1[p]$ and it is not a root of $X^{\frac{p-1}{2}}-1$ so $a^{\frac{p-1}{2}} \equiv -1[p]$.

QED.

Legendre symbol

Definition 3 (Legendre symbol) *For $p \in \mathbb{P}$, $p \leq 3$ and for $a \in \mathbb{Z}$, the Legendre symbol of a and p is:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0[p] \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p \\ 0 & \text{if } p \text{ divides } a \end{cases} \tag{51}$$

Using Euler's criterion it is possible to define a constructive definition of the Legendre symbol.

Theorem 14 (Legendre symbol with Euler's criterion) *With p an odd prime number and $a \in \mathbb{Z}$,*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p] \tag{52}$$

This definition leads to the multiplicative property of the Legendre symbol.

$$\forall (a,b) \in \mathbb{Z}^2, \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{53}$$

Gauss's lemma

Theorem 15 (Gauss's lemma) *With p an odd prime number and $a \in \mathbb{Z}$ coprime to p, let $S = \left\{a, 2a..., \frac{p-1}{2}a\right\}$. Each integer of S can be reduced modulo p in interval $\left[\!\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]\!\right]$. Let S' be the resulting set on reduced integers and n the number of negative numbers in S'.*

$$\left(\frac{a}{p}\right) = (-1)^n \tag{54}$$

Proof:

$$\left[\!\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]\!\right] = \left\{0, -1, 1, -2, 2..., -\frac{p-1}{2}, \frac{p-1}{2}\right\} \tag{55}$$

If $0 \in S'$, there is $ka \in S$ such that $ka \equiv 0[p]$. As $\gcd(a,p) = 1$, $k \equiv 0[p]$, which is impossible.

If there exists $x \in S'$ such that $-x \in S'$, there exist k, l such that

$$1 \leq k \leq \frac{p-1}{2} \tag{56}$$

$$1 \leq l \leq \frac{p-1}{2} \tag{57}$$

$$ka \equiv x[p] \tag{58}$$

$$la \equiv -x[p] \tag{59}$$

Therefore

$$2 \leq k + l \leq p - 1 \tag{60}$$

$$(k + l)a \equiv 0[p] \tag{61}$$

This is impossible.

Similarly, every element in S' is distinct. As S' contains $\frac{p-1}{2}$ elements, it can be rewritten as $\left\{\epsilon_1.1, \epsilon_2.2..., \epsilon_{\frac{p-1}{2}} \frac{p-1}{2}\right\}$, with $\epsilon_k \in \{-1, 1\}$.

The number of negative numbers in S' is the number of negative ϵ_k. Therefore

$$(-1)^n = \prod_{k=1}^{\frac{p-1}{2}} \epsilon_k \tag{62}$$

The product of items of S modulo p can be computed using two ways:

$$\prod_{s \in S} s \equiv \prod_{s \in S'} s[p] \tag{63}$$

$$\frac{p-1}{2}! a^{\frac{p-1}{2}} \equiv \frac{p-1}{2}! \prod_{k=1}^{\frac{p-1}{2}} \epsilon_k[p] \tag{64}$$

$$\left(\frac{a}{p}\right) = (-1)^n \tag{65}$$

QED.

Quadratic reciprocity

Theorem 16 (Law of quadratic reciprocity) *With p and q two distinct odd prime numbers*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{66}$$

Proof: Let's study the isomorphism from the Chinese Remainder Theorem (theorem 6):

$$\begin{array}{rccc} f: & (\mathbb{Z}/pq\mathbb{Z})^\times & \to & (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \\ & \bar{x} & \mapsto & \left(\overline{x \mod p}, \overline{x \mod q}\right) \end{array} \tag{67}$$

Let split each set into halves according to sign (when mapping items of $\mathbb{Z}/n\mathbb{Z}$ in $[\![-\frac{n-1}{2}, \frac{n-1}{2}]\!]$).

Let $U = \{f(1), f(-1)\} = \{(1,1),(-1,-1)\} \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. $(U,.)$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. The product of elements of $E = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times / U$ can be computed in several ways.

First, $E = \left\{\left(\overline{x \mod p}, \overline{x \mod q}\right) U, 1 \leq x \leq \frac{pq-1}{2} \wedge \gcd(x, pq) = 1\right\}$. The x which appear can be enumerated by skipping the multiples of p and q until $\frac{pq-1}{2}$.

$$\prod_{x=1,\gcd(x,pq)=1}^{\frac{pq-1}{2}} x \equiv \frac{\frac{pq-1}{2}!}{\left(p.2p...\frac{q-1}{2}p\right)\left(q.2q...\frac{p-1}{2}q\right)}[p] \tag{68}$$

$$\equiv \frac{(1.2..(p-1))\left((p+1)...(2p-1)\right)...\left(...(\frac{q-1}{2}p+\frac{p-1}{2})\right)}{q.2q...\frac{p-1}{2}q}[p] \tag{69}$$

$$\equiv \frac{(1.2..(p-1))\,(1...(p-1))\,...\,(1...(p-1))\left(1...\frac{p-1}{2}\right)}{\frac{p-1}{2}!q^{\frac{p-1}{2}}}[p] \tag{70}$$

$$\equiv \frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}}[p] \tag{71}$$

As $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right)[p]$, and its value is ± 1,

$$\prod_{x=1,\gcd(x,pq)=1}^{\frac{pq-1}{2}} x \equiv (p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right)[p] \tag{72}$$

Therefore,

$$\prod_{e\in E} e = \left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right) U \tag{73}$$

Second, E can also be split as $(\mathbb{Z}/p\mathbb{Z})^\times \times [\![1, \frac{q-1}{2}]\!]$:

$$\prod_{e\in E} e = \left((p-1)!^{\frac{q-1}{2}}, \left(\frac{q-1}{2}\right)!^{p-1}\right) U \tag{74}$$

The last factor can be rewritten:

$$\left(\frac{q-1}{2}\right)! \equiv \prod_{x=1}^{\frac{q-1}{2}} x[q] \tag{75}$$

$$\equiv \prod_{x=1}^{\frac{q-1}{2}} (-(q-x))\,[q] \tag{76}$$

$$\equiv (-1)^{\frac{q-1}{2}} \prod_{x=\frac{q+1}{2}}^{q-1} x[q] \tag{77}$$

$$\left(\frac{q-1}{2}\right)!\left(\frac{q-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}} \prod_{x=1}^{q-1} x[q] \tag{78}$$

$$\left(\frac{q-1}{2}\right)!^2 \equiv (-1)^{\frac{q-1}{2}}(q-1)![q] \tag{79}$$

$$\left(\frac{q-1}{2}\right)!^{p-1} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}}[q] \tag{80}$$

Therefore

$$\prod_{e\in E} e = \left((p-1)!^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}}\right) U \tag{81}$$

Combining these two ways leads to:

$$\left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right) U = \left((p-1)!^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}}\right) U \tag{82}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{83}$$

QED.

Square root of -1

Let p be an odd prime. -1 is a quadratic residue modulo p iff $\left(\frac{-1}{p}\right) = 1$. Using the definition of the Legendre symbol (theorem 14),

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}[p] \tag{84}$$

If $p \equiv 3[4]$, $\frac{p-1}{2}$ is odd so $(-1)^{\frac{p-1}{2}} = -1$ and -1 is a quadratic nonresidue. Otherwise, $p \equiv 1[4]$ because p is odd and -1 is a quadratic residue. In such a case, the square root of -1 can be computed using any non-quadratic residue x:

$$-1 = \left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} = x^{2\frac{p-1}{4}} = (x^{\frac{p-1}{4}})^2[p] \tag{85}$$

Theorem 17 (Square root of -1) *With $p \in \mathbb{P}$,*

- *If $p \equiv 0[2]$, $p = 2$ and $-1 \equiv 1[p]$ is a quadratic residue with one square root, itself.*
- *If $p \equiv 3[4]$, -1 is a quadratic nonresidue modulo p.*
- *If $p \equiv 1[4]$, -1 is a quadratic residue and its square roots are $\pm x^{\frac{p-1}{4}}$ mod p, with x being any quadratic nonresidue modulo p.*

Square root of 2

Let p be an odd prime. 2 is a quadratic residue modulo p iff $\left(\frac{2}{p}\right) = 1$.

Let's compute the Legendre symbol using Gauss's lemma. Let $S = 2, 4, 6..., p-1$ and S' the set of these integers reduced modulo p in $[\![-\frac{p-1}{2}, \frac{p-1}{2}]\!]$. Let n the number of negative integers in S'. Gauss's lemma states that:

$$\left(\frac{2}{p}\right) = (-1)^n \tag{86}$$

$$\begin{aligned} n &= |\{s \in S', s < 0\}| && (87)\\ &= \left|\left\{k \in [\![1, \frac{p-1}{2}]\!], \frac{p+1}{2} \leq 2k \mod p \leq p-1\right\}\right| && (88)\\ &= \left|\left[\!\left[\left\lceil \frac{p+1}{4} \right\rceil, \frac{p-1}{2}\right]\!\right]\right| && (89) \end{aligned}$$

The value of $(-1)^n$ depends on the value of $p \mod 8$. Let $2r + 1 = p \mod 8$ and a the quotient of the division of p by 8: $p = 8a + 2r + 1$.

$$\begin{aligned} n &= \left|\left[\!\left[\left\lceil 2a + \frac{r+1}{2} \right\rceil, 4a + r\right]\!\right]\right| && (90)\\ &= 4a + r + 1 - \left\lceil 2a + \frac{r+1}{2} \right\rceil && (91)\\ &\equiv r + 1 - \left\lceil \frac{r+1}{2} \right\rceil [2] && (92)\\ &\equiv \begin{cases} 0[2] \text{ if } r \equiv 0[4] \\ 1[2] \text{ if } r \equiv 1[4] \\ 1[2] \text{ if } r \equiv 2[4] \\ 0[2] \text{ if } r \equiv 3[4] \end{cases} && (93) \end{aligned}$$

Therefore:

$$\left(\frac{2}{p}\right) = (-1)^n = \begin{cases} 1 & \text{if } p \equiv 1[8] \\ -1 & \text{if } p \equiv 3[8] \\ -1 & \text{if } p \equiv 5[8] \\ 1 & \text{if } p \equiv 7[8] \end{cases} \tag{94}$$

Theorem 18 (Square root of -1) *With $p \in \mathbb{P}$,*

- *If $p \equiv 0[2]$, $p = 2$ and $2 \equiv 0[p]$ is a quadratic residue with one square root, itself.*
- *If $p \equiv 3[8]$ or $p \equiv 5[8]$, 2 is a quadratic nonresidue modulo p.*
- *If $p \equiv 1[8]$ or $p \equiv 7[8]$, 2 is a quadratic residue modulo p.*

Square root of simple cases

If $p \equiv 3[4]$,

$$\forall x \in (\mathbb{Z}/p\mathbb{Z})^\times, \left(\frac{x}{p}\right) = 1 \iff x^{\frac{p-1}{2}} \equiv 1[p] \tag{95}$$

$$\iff x^{\frac{p-1}{2}+1} \equiv x[p] \tag{96}$$

$$\iff x^{\frac{p+1}{4}.2} \equiv x[p] \tag{97}$$

$$\iff \left(x^{\frac{p+1}{4}}\right)^2 \equiv x[p] \tag{98}$$

If x is a quadratic residue modulo p, $x^{\frac{p+1}{4}}$ is a square root of x.

If $p \equiv 5[8]$, -1 is a residue modulo p and 2 is not. Let's define a square root of -1:

$$i := 2^{\frac{p-1}{4}} \mod p \tag{99}$$

For $x \in (\mathbb{Z}/p\mathbb{Z})^\times$,

$$\left(\frac{x}{p}\right) = 1 \iff x^{\frac{p-1}{2}} \equiv 1[p] \tag{100}$$

$$\iff \left(x^{\frac{p-1}{4}}\right)^2 \equiv 1[p] \tag{101}$$

$$\iff x^{\frac{p-1}{4}} \equiv 1[p] \vee x^{\frac{p-1}{4}} \equiv -1[p] \tag{102}$$

$$\iff x^{\frac{p+3}{4}} \equiv x[p] \vee -x^{\frac{p+3}{4}} \equiv x[p] \tag{103}$$

$$\iff \left(x^{\frac{p+3}{8}}\right)^2 \equiv x[p] \vee \left(ix^{\frac{p+3}{8}}\right)^2 \equiv x[p] \tag{104}$$

If x is a quadratic residue modulo p, either $x^{\frac{p+3}{8}}$ or $ix^{\frac{p+3}{8}}$ is a square root of x.

If $p \equiv 1[8]$, a more generic algorithm needs to be applied.

Cipolla's algorithm

Let p be an odd prime and x a non-null quadratic residue modulo p:

$$x^{\frac{p-1}{2}} \equiv 1[p] \tag{105}$$

The aim of Cipolla's algorithm is to compute $r \in \mathbb{Z}$ such that $r^2 \equiv x[p]$.

Let's find $a \in [\![1, p-1]\!]$ such that $a^2 - x$ is a quadratic non-residue modulo p:

$$\left(a^2 - x\right)^{\frac{p-1}{2}} \equiv -1[p] \tag{106}$$

This can be done in a random way because there are $\frac{p-1}{2}$ such numbers.

Let $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2 - a^2 + x)$ be a set where elements are represented by $x + y\sqrt{a^2 - x}$, with $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2$. $(\mathbb{F}_{p^2}, +, .)$ is a finite field. Therefore if $\pm r$ are the roots of $X^2 - x$ in $\mathbb{Z}/p\mathbb{Z}$, they are also the roots (and there are only these two ones) of this polynomial in $\mathbb{F}_{p^2}$.

It is possible to compute in $\mathbb{F}_{p^2}$:

$$r := \left(a + \sqrt{a^2 - x}\right)^{\frac{p+1}{2}} \tag{107}$$

Let's show that $r^2 = x$ in $\mathbb{F}_{p^2}$.

Let $\omega = \sqrt{a^2 - x} \in \mathbb{F}_{p^2}$.

$$\omega^{p-1} = \left(\omega^2\right)^{\frac{p-1}{2}} = \left(a^2 - x\right)^{\frac{p-1}{2}} = -1 \text{ in } \mathbb{F}_{p^2} \tag{108}$$

$$\begin{aligned}
r^2 &= (a+\omega)^{\frac{p+1}{2}.2} && (109)\\
&= (a+\omega)^{p+1} && (110)\\
&= (a+\omega)(a+\omega)^p && (111)\\
&= (a+\omega)(a^p + \omega^p) \text{ because } p = 0 \text{ in } \mathbb{F}_{p^2} && (112)\\
&= (a+\omega)(a-\omega) \text{ because } a^{p-1} = 1 \text{ and } \omega^{p-1} = -1 && (113)\\
&= a^2 - \omega^2 && (114)\\
&= a^2 - (a^2 - x) && (115)\\
&= x && (116)
\end{aligned}$$

As $\mathbb{F}_{p^2}$ is a field, $X^2 - x$ only has two roots in it, which are therefore $\pm r$. This polynomial also has roots in $\mathbb{Z}/p\mathbb{Z}$ and any root in it has to be a root in $\mathbb{F}_{p^2}$. This is why $r \in \mathbb{Z}/p\mathbb{Z}$.

To conclude, this algorithm built a square root (r) of x modulo p.

Arithmetic modulo a power of 2

Basic properties

When working with numbers on a computer, it is quite common to work modulo a power of 2, like 2^{16}, 2^{32} or 2^{64}. There are some interesting properties in such computations, that can be used in several algorithms.

Let $N \in \mathbb{N}^*$ be the number of bits which is considered. The remaining of this part will focus on working in $\mathbb{Z}/2^N\mathbb{Z}$.

- If $N = 1$, $\mathbb{Z}/2\mathbb{Z}$ is a field containing to items, $\{0, 1\}$, and it is not much interesting.
- If $N = 2$, $\mathbb{Z}/4\mathbb{Z}$ is a ring that contains two invertible items, 1 and $3 = -1$.

It becomes more generic when N is larger, for example when $N \in \{16, 32, 64\}$.

Let's begin with a theorem which comes from the fact that 2 is the only prime divisor of 2^N.

Theorem 19 (invertible items modulo 2^N) *The set of the numbers invertible modulo 2^N is the set of odd numbers.*

As there are 2^{N-1} odd numbers in $\mathbb{Z}/2^N\mathbb{Z}$, the Euler totient function on 2^N is:

$$\phi(2^N) = 2^{N-1} \tag{117}$$

This can also be computed thanks to the formula $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Then using Euler's theorem,

Theorem 20 (Euler's theorem in $\mathbb{Z}/2^N\mathbb{Z}$)

$$\forall x \text{ odd number }, x^{2^{N-1}} \equiv 1[2^N] \tag{118}$$

Quadratic residues modulo a power of 2

When analyzing the squares, here is a formula which has some consequences, when $N \geq 2$:

$$\forall r \in \mathbb{Z}, (2^{N-1} + r)^2 = 2^{2N-2} + 2^N r + r^2 \equiv r^2[2^N] \tag{119}$$

This means that if r is a square root of a modulo 2^N, $2^{N-1} + r$ is also a square root, and so is its opposites $2^N - (2^{N-1} + r) = 2^{N-1} - r$. Moreover when a is odd, r must be too, so r cannot be 0 nor 2^{N-1}. Therefore an odd quadratic residue has at least 4 roots modulo 2^N when $N \geq 3$ (the three that where given and $-r$).

Another formula is:

$$\forall x \in \mathbb{Z}, (2x+1)^2 = 4x^2 + 4x + 1 = 4x(x+1) + 1 \equiv 1[8] \tag{120}$$

Moreover 8 divides 2^N if $N \geq 3$ and the result is trivial for $N < 3$. Therefore all odd quadratic residues in $\mathbb{Z}/2^N\mathbb{Z}$ are congruent to 1 modulo 8.

From now on, let's consider $N \geq 3$. Let f be the square function restricted to the invertible items of $\mathbb{Z}/2^N\mathbb{Z}$ (which are the odd numbers $(2\mathbb{Z}+1)/2^N\mathbb{Z}$):

$$f : (\mathbb{Z}/2^N\mathbb{Z})^\times \rightarrow (8\mathbb{Z}+1)/2^N\mathbb{Z} = \{x \in \mathbb{Z}/2^N\mathbb{Z}, x \equiv 1[8]\} \tag{121}$$

$$r \mapsto r^2 \tag{122}$$

As it was shown that $f(r) = f(2^{N-1} - r) = f(2^{N-1} + r) = f(2^N - r)$, it is possible to restrict further f to the set of odd numbers between 0 and 2^{N-2} (i.e. $(2\mathbb{Z}+1) \cap [\![1, 2^{N-2} - 1]\!]$). Let's prove that this restricted f is injective. If r_1 and r_2 are two numbers such that $0 < r_2 < r_1 < 2^{N-2}$ and $f(r_1) = f(r_2)$. $r_1^2 \equiv r_2^2[2^N]$ so:

$$(r_1 - r_2)(r_1 + r_2) \equiv 0[2^N] \tag{123}$$

As $r_1 - r_2 \neq 0[2^N]$, let p be the power of 2 of the prime decomposition of $r_1 - r_2$. This means that $0 \leq p \leq N-1$, 2^p divides $(r_1 - r_2)$ and 2^{p+1} does not. As r_1 and r_2 are odd, $p \geq 1$. As $0 < r_2 < r_1 < 2^{N-2}$, $0 < r_1 - r_2 < 2^{N-2}$ so $p < N-2$. Let α be the odd number such that $r_1 - r_2 = \alpha 2^p$.

$$2^N \text{ divides } (r_1 - r_2)(r_1 + r_2) = \alpha 2^p(2r_2 + \alpha 2^p) \tag{124}$$

$$2^{N-p} \text{ divides } \alpha \times 2(r_2 + \alpha 2^{p-1}) \tag{125}$$

$$2^{N-p-1} \text{ divides } r_2 + \alpha 2^{p-1} \tag{126}$$

As $p < N-2$, 2^{N-p-1} is even and the only way for the right member to be even (with r_2 and α being odd) is when $2^{p-1} = 1$. Therefore p must be 1, which means that 2^{N-2} divides $r_2 + \alpha \neq 0$ and $0 < r_1 = r_2 + 2\alpha < 2^{N-2}$, which is impossible.

Therefore the hypothesis leading to the definition of r_1 and r_2 is absurd and f is injective from the set of odd numbers between 0 and 2^{N-2}. There are $\frac{2^{N-2}}{2} = 2^{N-3}$ such numbers. This is also the cardinality of $(8\mathbb{Z}+1)/2^N\mathbb{Z}$. Therefore the restricted f is bijective, which means that every number in $(8\mathbb{Z}+1)/2^N\mathbb{Z}$ is a square residue.

Theorem 21 (Odd quadartic residues modulo 2^N) *An odd number x is a quadratic residue modulo 2^N if and only if $x \equiv 1[8]$. It then has four square roots that can be computed from one (modulo 2^N): r, $2^{N-1} - r$, $2^{N-1} + r$ and $2^N - r$.*

For example, the square roots of 1 are 1, $2^{N-1} - 1$, $2^{N-1} + 1$ and $2^N - 1$.

It would be nice to have something like the Legendre symbol to characterize quadratic residues, which only works when the modulus is a prime number, but

it does not work for example with $N = 4$: modulo 16, 1 and 9 are the only odd quadratic residues and the order of the group is 4 ($x^4 \equiv 1[16]$ for x odd).

Nevertheless the last result can be used to refine the equation given by Euler's theorem. As the set of quadratic residues modulo 2^N (written $(8\mathbb{Z}+1)/2^N\mathbb{Z}$) is stable through multiplication and inversion, it is a commutative group. Its cardinal is 2^{N-3}, therefore the Lagrange theorem gives:

Theorem 22 (Refined Euler's theorem modulo 2^N) *With $N \geq 3$,*

$$\forall x \in \mathbb{Z}, x \equiv 1[8] \quad \Rightarrow \quad x^{2^{N-3}} \equiv 1[2^N] \tag{127}$$

$$\forall r \in \mathbb{Z}, r \equiv 1[2] \quad \Rightarrow \quad r^{2^{N-2}} \equiv 1[2^N] \tag{128}$$

When studying an even number, its decomposition as a product of an odd number and a power of two $\alpha 2^p$ allows to work out a simple rule about even quadratic residues. If 2 is a quadratic residue modulo 2^N, there exists $r \in \mathbb{Z}$ such that

$$r^2 \quad \equiv \quad 2[2^N] \tag{129}$$

$$2^N \quad \text{divides} \quad r^2 - 2 \tag{130}$$

$$2 \text{ divides } r^2 \quad \text{and} \quad 2^{N-1} \text{ divides } \frac{r^2}{2} - 1 \tag{131}$$

$$2 \text{ divides } r \quad \text{and} \quad 2^{N-1} \text{ divides } 2\left(\frac{r}{2}\right)^2 - 1 \tag{132}$$

$$\tag{133}$$

This would only be possible with $2^{N-1} = 1$, i.e. $N = 1$ and $2^N = 2$ (and then the square root of 2 is 0). When $N \geq 2$, 2 is not a quadratic residue, so there is a simple rule:

Theorem 23 (Generic quadartic residues modulo 2^N) *A number decomposed as $\alpha 2^p$ with α odd and $p \in \mathbb{N}$ is a quadratic residue modulo 2^N if and only if either $p \geq N$ or $\alpha \equiv 1[8]$ and p is even.*

Square roots modulo a power of 2

Theorem 21 can be used to design an algorithm that computes square roots of odd numbers. For all $x \in 8\mathbb{Z}+1$ (i.e. such that $x \equiv 1[8]$), x has a square root modulo 2^N whatever N is.

- If $N \leq 3$, $2^N \in \{1, 2, 4, 8\}$ and $x \equiv 1[2^N]$ therefore the square roots of x modulo 2^N are 1, 3, 5 and 7 (some of these numbers being equivalent modulo 2^N when $N < 3$).
- When $N \geq 3$, x has 4 distinct square roots modulo 2^N, one of them lying between 0 and 2^{N-2} (excluded). Let $sqrt_N(x)$ be this value.

Definition 4 (Square root function modulo 2^N) *For all $N \geq 3$, the square root function modulo 2^N is defined as:*

$$\begin{aligned} sqrt_N : 8\mathbb{Z}+1 &\rightarrow \mathbb{Z} && (134)\\ x &\mapsto r : 0 < r < 2^{N-2} \wedge r^2 \equiv x[2^N] && (135)\end{aligned}$$

This definition can be extended to $N \leq 2$ with $sqrt_1(x) = sqrt_2(x) = 1$

It is trivial to compute $sqrt_N(1) = 1$.

With $N \geq 3$, x has four square roots modulo N: $sqrt_N(x)$, $2^{N-1} - sqrt_N(x)$, $2^{N-1} + sqrt_N(x)$ and $2^N - sqrt_N(x)$. These roots are sorted:

$$0 < sqrt_N(x) < 2^{N-2} < 2^{N-1} - sqrt_N(x) < 2^{N-1} \quad (136)$$

$$2^{N-1} < 2^{N-1} + sqrt_N(x) < 3 \times 2^{N-2} < 2^N - sqrt_N(x) < 2^N \quad (137)$$

When $sqrt_N(x)$ is known, how could $sqrt_{N+1}(x)$ be computed? There exist some relationships:

$$\begin{aligned} sqrt_{N+1}(x)^2 &\equiv x[2^{N+1}] && (138)\\ sqrt_{N+1}(x)^2 &\equiv x[2^N] && (139)\end{aligned}$$

$$sqrt_{N+1}(x) \in \left\{\pm sqrt_N(x), 2^{N-1} \pm sqrt_N(x)\right\} \text{ modulo } 2^N \quad (140)$$

As $0 < sqrt_{N+1}(x) < 2^{N+1-2} = 2^{N-1}$, this leads to:

$$sqrt_{N+1}(x) \in \left\{sqrt_N(x), 2^{N-1} - sqrt_N(x)\right\} \text{ (in } \mathbb{Z}) \quad (141)$$

Moreover, using that $sqrt_N(x)$ is odd,

$$\begin{aligned} \left(2^{N-1} - sqrt_N(x)\right)^2 &= 2^{2N-2} - 2^N sqrt_N(x) + sqrt_N(x)^2 && (142)\\ \left(2^{N-1} - sqrt_N(x)\right)^2 &\equiv -2^N + sqrt_N(x)^2[2^{N+1}] && (143)\\ \left(2^{N-1} - sqrt_N(x)\right)^2 + 2^N &\equiv sqrt_N(x)^2[2^{N+1}] && (144)\end{aligned}$$

Therefore:

- If $sqrt_{N+1}(x) = sqrt_N(x)$, $sqrt_N(x)^2 = sqrt_{N+1}(x)^2 \equiv x[2^{N+1}]$.
- Otherwise $sqrt_{N+1}(x) = 2^{N-1} - sqrt_N(x)$ and

$$\begin{aligned} sqrt_N(x)^2 &\equiv 2^N + \left(2^{N-1} - sqrt_N(x)\right)^2 [2^{N+1}] && (145)\\ sqrt_N(x)^2 &\equiv 2^N + x[2^{N+1}] && (146)\end{aligned}$$

By reversing the conditions, the following theorem is proven

Theorem 24 (Recursive computation of the square root function 2^N) *The square root function modulo 2^N can be recursively defined on $x \in 8\mathbb{Z}+1$ by:*

$$\forall N \leq 3, sqrt_N(x) = 1 \tag{147}$$

$$\forall N \geq 4, sqrt_N(x) = \begin{cases} sqrt_{N-1}(x) & if \quad sqrt_{N-1}(x)^2 \equiv x[2^N] \\ 2^{N-2} - sqrt_{N-1}(x) & if \quad sqrt_{N-1}(x)^2 \equiv 2^{N-1} + x[2^N] \end{cases} \tag{148}$$

There is no third case.

Here are some values in hexadecimal:

- $\forall N \geq 4, sqrt_N(9) = 3$
- $sqrt_{64}(17) =$ 0x5a241f333d326e9
- $\forall N \geq 5, sqrt_N(25) = 5$
- $sqrt_{64}(33) =$ 0x3289350725bd6791
- $sqrt_{64}(41) =$ 0x1b226bfe00cc66cd

Quadratic equation modulo a power of 2

Let's consider the following equation ($N \in \mathbb{N}, a, b, c, x \in \mathbb{Z}$):

$$ax^2 + bx + c \equiv 0[2^N] \tag{149}$$

If $N = 0$, every number is a solution. Let's suppose that $N \geq 1$. If x is a solution, $x + 2^N$ too. Therefore the set of solutions can be written as a set of items from $\mathbb{Z}/2^N\mathbb{Z}$.

Depending on the parity of a, b and c, the result is different:

- If a, b and c are even, the equation is equivalent to one with each term divided by 2 and N replaced by $N-1$.
- If a and b are even but not c, there is no solution when $N \geq 1$.
- If a is odd, a is invertible modulo 2^N so the equation is equivalent to one with $a = 1$.
  - If $a = 1$ and $b = 0$, the solutions are the 4 square roots of $-c$ if $-c \equiv 1[8]$, otherwise there is no solution.
  - If b is even, the equation can be factorized as $\left(x + \frac{b}{2a}\right)^2 \equiv \frac{b^2-4ac}{4a^2}[2^N]$ (the divisions hold because the values have the right parity or are invertible), which goes back to the previous case. Depending on the values, there may be 0 or 4 solutions to the equation.
  - If b is odd too, the analysis becomes quite complex.

- If a and even and b is odd, let's prove there is only one solution. If x_1 and x_2 are two solutions,

$$\begin{aligned} ax_1^2 + bx_1 &\equiv ax_2^2 + bx_2[2^N] && (150)\\ (a(x_1+x_2)+b)(x_1-x_2) &\equiv 0[2^N] && (151)\\ & && (152) \end{aligned}$$

$$\begin{aligned} 2^N \quad \text{divides} \quad & (a(x_1+x_2)+b)(x_1-x_2) && (153)\\ 2^N \quad \text{divides} \quad & (x_1-x_2) \text{ (as } a(x_1+x_2)+b \text{ is odd)} && (154)\\ x_1 \quad \equiv \quad & x_2[2^N] && (155) \end{aligned}$$

  Therefore there is at most one solution. By studying the function $x \mapsto ax^2 + bx$ from and to $\mathbb{Z}/2^N\mathbb{Z}$, this function is injective so it is bijective. This means that the initial equation has one and only one solution, which is the preimage of $-c$ by the function.

If the working set was the set of complex numbers $\mathbb{C}$, the equation would always have two solutions defined by:

$$\begin{aligned} \Delta &= b^2 - 4ac && (156)\\ x_1, x_2 &= \frac{-b \pm \sqrt{\Delta}}{2a} && (157) \end{aligned}$$

This is because the equation would be factorized as:

$$a(x - x_1)(x - x_2) = 0 \tag{158}$$

Here, this way of solving the equation cannot be applied exactly as it is, at least because the equation may have 4 solutions, or none, or one...

If a is odd and b is even, changing variable to $y \equiv x + \frac{b}{2}a^{-1}[2^N]$ and defining Δ, the equation becomes $y^2 \equiv \frac{\Delta}{4}(a^{-1})^2[2^N]$, or $(ay)^2 \equiv \frac{\Delta}{4}[2^N]$.

- If $\frac{\Delta}{4} \equiv 1[8]$, $\frac{\Delta}{4}$ has 4 roots modulo 2^N and if r is one of them, $x \equiv \left(r - \frac{b}{2}\right)a^{-1}[2^N]$ is a solution of the equation $ax^2 + bx + c \equiv 0[2^N]$. It can be shown that the equation only has these 4 solutions.
- Otherwise, $\frac{\Delta}{4}$ is not a quadratic residue and the equation does not have any solution.

If a is even and b is odd, it has been shown that the equation has a unique solution. Moreover,

$$\begin{aligned} 4a &\equiv 0[8] && (159)\\ \Delta = b^2 - 4ac &\equiv b^2 \equiv 1[8] && (160) \end{aligned}$$

Therefore Δ is a quadratic residue (whatever the value of c) and has 4 square roots modulo 2^N which are all odd. Nevertheless, these roots are not those which will be needed. Here is what the equation becomes:

$$\begin{aligned}
0 &\equiv ax^2+bx+c[2^N] && (161)\\
4a\times 2^N &\text{ divides } (2ax)^2+4abx+4ac && (162)\\
4a\times 2^N &\text{ divides } (2ax+b)^2-(b^2-4ac) && (163)\\
4a\times 2^N &\text{ divides } (2ax+b)^2-\Delta && (164)
\end{aligned}$$

In order to transform Δ to δ^2, the squaring root operation could need to be done modulo $4a\times 2^N$, which is quite inconvenient. It is nonetheless possible to reduce this equation to a squaring root modulo a power of two. Let's define α and p such that $a=\alpha 2^{p+1}$ with α odd. Let α^{-1} be the inverse of α modulo 2^{N+p+3}. The equation becomes:

$$\begin{aligned}
4a\times 2^N &\text{ divides } (2ax+b)^2-\Delta && (165)\\
4\alpha 2^{p+1}\times 2^N &\text{ divides } (2ax+b)^2-\Delta && (166)\\
\left(\alpha^{-1}\right)^2\alpha\times 2^{N+p+3} &\text{ divides } \left(\alpha^{-1}\right)^2(2ax+b)^2-\left(\alpha^{-1}\right)^2\Delta && (167)\\
2^{N+p+3} &\text{ divides } \left(2\times 2^{p+1}x+\alpha^{-1}b\right)^2-\left(\alpha^{-1}\right)^2\Delta && (168)
\end{aligned}$$

Let δ be a square root of Δ modulo 2^{N+p+3}. The four square roots of Δ are then $\pm\delta$ and $2^{N-1}\pm\delta$. With δ being one of these roots:

$$\begin{aligned}
2^{N+p+3} &\text{ divides } \left(2\times 2^{p+1}x+\alpha^{-1}b\right)^2-\left(\alpha^{-1}\right)^2\Delta && (169)\\
2^{N+p+3} &\text{ divides } \left(2^{p+2}x-\alpha^{-1}(-b)\right)^2-\left(\alpha^{-1}\right)^2\delta^2 && (170)\\
2^{N+p+3} &\text{ divides } \left(2^{p+2}x-\alpha^{-1}(-b+\delta)\right)\left(2^{p+2}x-\alpha^{-1}(-b-\delta)\right) && (171)
\end{aligned}$$

$-b\pm\delta$ are even so can be divided by 2. In order to "divide it by 2^{p+1} too", let's choose δ such that $-b+\delta\equiv 0[4]$. If it is not the case, it will be the case with using $-\delta$ (because b and δ are both odd).

$$\begin{aligned}
2^{N+p+3} &\text{ divides } \left(2^{p+2}x-\alpha^{-1}(-b+\delta)\right)\left(2^{p+2}x-\alpha^{-1}(-b-\delta)\right) && (172)\\
2^{N+p+1} &\text{ divides } \left(2^{p+1}x-\frac{-b+\delta}{2}\alpha^{-1}\right)\left(2^{p+1}x-\frac{-b-\delta}{2}\alpha^{-1}\right) && (173)\\
2^{N+p+1} &\text{ divides } 2^{p+1}x-\frac{-b+\delta}{2}\alpha^{-1} && (174)\\
&\text{because } \frac{-b-\delta}{2} \text{ and } \alpha^{-1} \text{ are odd} && (175)\\
2^N &\text{ divides } x-\frac{-b+\delta}{2^{p+2}}\alpha^{-1} && (176)\\
x &\equiv \frac{-b+\delta}{2^{p+2}}\alpha^{-1}[2^N] && (177)\\
& && (178)
\end{aligned}$$

This is indeed a way to write $\frac{-b\pm\sqrt{\Delta}}{2a}$ which is possible to compute modulo 2^N in this case ($\pm\sqrt{\Delta}$ being a square root of Δ modulo 2^{N+p+3} such that $\delta\equiv b[4]$).