Alexander Rostovtsev,
St. Petersburg State Polytechnic University
rostovtsev@ssl.stu.neva.ru

Fast exponentiation via prime finite field isomorphism

Raising of the fixed element of prime order group to arbitrary degree is the main operation specified by digital signature algorithms DSA, ECDSA. Fast exponentiation algorithms are proposed. Algorithms use number system with algebraic integer base $\sqrt[4]{\pm 2}$. Prime group order r can be factored $r = \pi\bar{\pi}$ in Euclidean ring $\mathbb{Z}[\sqrt{\pm 2}]$ by Pollard and Schnorr algorithm. Farther factorization of prime quadratic integer $\pi = \rho\bar{\rho}$ in the ring $\mathbb{Z}[\sqrt[4]{\pm 2}]$ can be done similarly. Finite field $\mathbb{F}_r$ is represented as quotient ring $\mathbb{Z}[\sqrt[4]{\pm 2}]/(\rho)$. Integer exponent k is reduced in corresponding quotient ring by minimization of absolute value of its norm. Algorithms can be used for fast exponentiation in arbitrary cyclic group if its order can be factored in corresponding number rings. If window size is 4 bits, this approach allows speeding-up 2.5 times elliptic curve digital signature verification comparatively to known methods with the same window size.

Key words: fast exponentiation, cyclic group, algebraic integers, digital signature, elliptic curve.

1. Introduction

Let G be cyclic group of prime computable order. Raising of the fixed element $a \in G$ to arbitrary degree is the main operation specified by many public key cryptosystems, such as digital signature algorithms DSA, ECDSA [2]. In cryptographic applications prime group order is more then 2^{100}. Group G can be given as subgroup of finite field [6], elliptic curve or Jacobian of hyperelliptic curve over finite field, class group of number field, etc. Group operation can be called both addition (additive group) or multiplication (multiplicative group). In additive group raising element a to exponent k is denoted as ka (scalar multiplication), in multiplicative group it is denoted as a^k.

Let $r \in \mathbb{Z}_{>0}$ be prime order of additive group G and $a \in G$. The general method for computing multiple $b = ka$ takes binary representation of the exponent $k = \sum_{i=0}^{N} k_i 2^i$ [4, 6]. Let $b_N = 0$ and for $i = N - 1, N - 2, \ldots, 0$ compute $b_j = 2b_{j+1}$ if $k_i = 0$ and $b_i = 2b_{i+1} + a$ if $k_i = 1$. This method at average takes $\log_2 r$ doublings and $0.5 \cdot \log_2 r$ additions.

There is natural way to speed-up this method slightly if element a is fixed. Choose window size w bits and compute base $\{a, 2a, \ldots, (2^w - 1)a\}$ (since element a is fixed, this base can be stored in computer memory). Transition to next window takes w doublings and one addition, so exponentiation takes $\log_2 r$ doublings and $(\log_2 r)/w$ additions. Note that size of the base grows as exponent of w, so window size cannot be large in practice. If $w = 4$ and complexities of doubling and addition are equal, this gives speeding-up about 20% with respect to previous method.

Elliptic curves over prime finite fields belong to the set of most popular mathematical structures in public key cryptology. For example, elliptic curve digital signature algorithm ECDSA and some national digital signature standards use such elliptic curves.

The most difficult operation during signature generation and verification is (scalar) multiplication of the elliptic curve point by a number, that corresponds to exponentiation.

Let $p > 3$ be a prime, $\mathbb{F}_p$ — prime finite field and

$$E(\mathbb{F}_p)\colon Y^2Z = X^3 + AXZ^2 + BZ^3 \tag{1}$$

— Weierstrass equation for elliptic curve. Set of points $(X, Y, Z)\backslash(0, 0, 0)$, where $(X, Y, Z) = (uX, uY, uZ)$ for any $u \neq 0$, form additive Abelian group with zero element $P_\infty = (0, 1, 0)$, and $-(X, Y, Z) = (X, -Y, Z)$.

Elliptic curve up to isomorphism over quadratic extension of prime field is uniquely determined by its invariant $j = \dfrac{12^3 \cdot 4A^3}{4A^3 + 27B^2}$. Elliptic curve arithmetic is given by polynomials over $\mathbb{F}_p$. If $(X_3, Y_3, Z_3) = 2(X_1, Y_1, Z_1)$, then

$$X_3 \equiv 2Y_1Z_1((3X_1^2 + AZ_1^2)^2 - 8X_1Y_1^2Z_1),$$
$$Y_3 \equiv 4Y_1^2Z_1(3X_1(3X_1^2 + AZ_1^2) - 2Y_1^2Z_1) - (3X_1^2 + AZ_1^2)^3,$$
$$Z_3 \equiv 8Y_1^3Z_1^3.$$

If $(X_3, Y_3, Z_3) = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)$, then

$$X_3 \equiv (X_2Z_1 - X_1Z_2)(Z_1Z_2(Y_2Z_1 - Y_1Z_2)^2 - (X_2Z_1 + X_1Z_2)(X_2Z_1 - X_1Z_2)^2),$$
$$Y_3 \equiv (X_2Z_1 - X_1Z_2)^2(Y_2Z_1(X_2Z_1 + 2X_1Z_2) - Y_1Z_2(X_1Z_2 + 2X_2Z_1)) - Z_1Z_2(Y_2Z_1 - Y_1Z_2)^3,$$
$$Z_3 \equiv Z_1Z_2\,(X_2Z_1 - X_1Z_2)^3.$$

Elliptic curve isomorphisms are given by maps: $(A, B, X, Y) \leftarrow (u^4A, u^6B, u^2X, u^3Y)$. If $p \equiv 3 \pmod 4$, then using suitable isomorphism one can obtain $A = \pm 1$.

The most difficult operation during elliptic curve point exponentiation is modular multiplication, so complexity of elliptic curve digital signature algorithms can be estimated as number of required modular multiplications. Point doubling takes 13 modular multiplications, point addition takes 15 modular multiplications. If addend point has $Z_1 = 1$ (this often holds in practice), then 12 modular multiplications are needed for point addition.

Some specific groups admit additional exponentiation methods. For example, if G is elliptic curve over finite field, then for any point $P \in G$ its negative $-P$ can be computed easily comparatively to point doubling or point addition operations. This allows using exponent representation in number system with elements $(-1, 0, 1\}$. Hence chains of kind 0, 1, 1, …, 1, 1 can be changed by chains 1, 0, 0, …, 0, –1 with reduced number of non-zero digits (at average from $N/2$ to $N/3$). If window size is 1 bit, this allows speeding-up exponentiation about 10%. But for larger window sizes speeding-up is negligible.

If there exists element $\sqrt{-2} \pmod{p}$ and $j = 20^3$, then elliptic curve is isomorphic to curve $Y^2Z = X^3 - 4tX^2Z + 2t^2XZ^2$. Transition to equation (1) is given by changing $X \leftarrow X + \frac{4tZ}{3}$, $A = \frac{-10t^2}{3}$, $B = \frac{-56t^3}{27}$. This elliptic curve has complex multiplication by $\sqrt{-2}$:

$$\sqrt{-2}(X,Y,Z) = \left(-Y^2Z,\ \frac{Y(X^2 - 2t^2Z^2)}{\sqrt{-2}},\ 2X^2Z \right).$$

Elliptic curve complex multiplication takes 7 modular multiplications. Using complex multiplication instead or with point doubling gives additional acceleration [8]. Sometimes using Hesse equation for elliptic curve allows slightly (about 1.3 times) speed-up point doubling and point addition [3]. But complex multiplication formula for such equation is inconvenient.

Cryptosystem parameters include elliptic curve $E(\mathbb{F}_p)$, point Q of prime order r, secret key l and public key $P = lQ$. Signature generation takes computing point $R = kQ$ for random k. Signature verification takes multiplication of both fixed points Q, P by exponents.

The purpose of this paper is to propose new fast exponentiation method based on number system with algebraic integer base $\sqrt{\pm 2}$ or $\sqrt[4]{\pm 2}$ and window size two or four bits. Then transition to next window takes only one doubling (comparatively to two or four doublings in known methods). This gives significant acceleration (more then two times) with respect to known methods. Algorithms can be used for fast exponentiation in arbitrary cyclic group if its order can be factored in corresponding number rings.

2. Algebraic basics

Number fields $\mathbb{Q}[\sqrt{\pm 2}], \mathbb{Q}[\sqrt[4]{\pm 2}]$ have rings of integers $\mathbb{Z}[\sqrt{\pm 2}], \mathbb{Z}[\sqrt[4]{\pm 2}]$ respectively. These rings are Euclidean [5] and hence possess unique factorization property. Group of units is finite for ring $\mathbb{Z}[\sqrt{-2}]$ and is infinite for three other rings: in $\mathbb{Z}[\sqrt{2}]$ free group of units is generated by number $1 + \sqrt{-2}$, in $\mathbb{Z}[\sqrt[4]{-2}]$ this group is generated by number $1 + 2\sqrt[4]{-2} - \sqrt{-2}$, in $\mathbb{Z}[\sqrt[4]{2}]$ this group is generated by numbers $1 + \sqrt[4]{2}$ and $1 - \sqrt[4]{2}$ [1].±

Field $\mathbb{Q}[\sqrt[4]{\pm 2}]$ and its ring of integers is quadratic extension of field $\mathbb{Q}[\sqrt{\pm 2}]$ and its ring of integers. Galois group of field $\mathbb{Q}[\sqrt[4]{\pm 2}]$ over $\mathbb{Q}$ is cyclic of order 4, it is generated by automorphism $\sigma(\sqrt[4]{\pm 2}) = i\sqrt[4]{\pm 2}$, where $i^2 = -1$. In spite of $i \notin \mathbb{Q}[\sqrt[4]{\pm 2}]$, norm of algebraic number from field $\mathbb{Q}[\sqrt[4]{\pm 2}]$ into its subfields can be defined.

Norms of quadratic numbers $a+b\sqrt{-2}$, $a+b\sqrt{2}$ in $\mathbb{Q}$ are $a^2 + 2b^2$, $a^2 - 2b^2$ respectively. Norm of algebraic number $\xi = a_0 + a_1\sqrt[4]{\pm 2} + a_2\sqrt[4]{\pm 2}^2 + a_3\sqrt[4]{\pm 2}^3$ in $\mathbb{Q}[\sqrt{\pm 2}]$ is $\xi\cdot\sigma^2(\xi)$, and its norm in field $\mathbb{Q}$ is $\xi\cdot\sigma(\xi)\cdot\sigma^2(\xi)\cdot\sigma^3(\xi)$.

Let $K = \mathbb{Q}[z]/(f(z))$ is number field, obtained by adjoining root α of irreducible polynomial $f(z)$ and O_K is Euclidean ring of integers in field K. Prime r splits in O_K, if $f(z)$ has root (and hence splits completely) modulo r. Element $\alpha \pmod r$ is one of roots of $f(z)$ modulo r. One can choose this root ρ so that congruence $\rho \equiv 0 \pmod r$ holds. Changing element α by a root of the polynomial gives homomorphism $O_K \to \mathbb{F}_r$. Prime algebraic integer ρ generates maximal ideal (ρ), so there exists isomorphism of prime finite fields $\mathbb{F}_r \cong O_K/(\rho)$.

Proposed algorithms for raising to power k use finite field representation $\mathbb{F}_r \cong O_K/(\rho)$ and exponent k representation as element of $O_K/(\rho)$. Element of $O_K/(\rho)$ is residue class of algebraic integers. Congruence $k \equiv k + \beta\rho \pmod\rho$ holds for any $\beta \in O_K$. Chose algebraic integer β so that absolute norm of $k + \beta\rho$ is minimal.

Isomorphism $\mathbb{F}_r \cong O_K/(\rho)$ for fields $\mathbb{Q}[\sqrt{\pm 2}], \mathbb{Q}[\sqrt[4]{\pm 2}]$ is computable in both directions: to compute $O_K/(\rho) \to \mathbb{F}_r$ substitute $\alpha \to \alpha \pmod r$. Consider inverse isomorphism.

Rings $\mathbb{Z}[\sqrt{\pm 2}]$, $\mathbb{Z}[\sqrt[4]{\pm 2}]$ are Euclidean over $\mathbb{Z}$ [5], division is defined by minimization of absolute value of the norm. Since norm from $\mathbb{Z}[\sqrt[4]{\pm 2}]$ to $\mathbb{Z}[\sqrt{\pm 2}]$ is defined by subgroup of Galois group, rings $\mathbb{Z}[\sqrt[4]{\pm 2}]$ are Euclidean over $\mathbb{Z}[\sqrt{\pm 2}]$.

Prime r such that $\left(\frac{-2}{r}\right) = 1$ can be factored in imaginary quadratic order by algorithm of Pollard and Schnorr [7], which is similar to extended Euclidean algorithm.

Algorithm 1. Prime integer factorization in imaginary quadratic order.
Input. Prime r.
Output. Numbers a, b such that $r = a^2 + 2b^2$.
Method.

1. Compute Jacobi symbol $\left(\frac{-2}{r}\right)$. If it is –1, then there are no solutions.
2. Compute $u \leftarrow \sqrt{-2} \pmod r$, for example by algorithm in [6].
3. $i \leftarrow 0$, $u_i \leftarrow u$, $m_i \leftarrow r$.
4. Compute

$$m_{i+1} \leftarrow \frac{u_i^2 + 2}{m_i},$$

$$u_{i+1} \leftarrow \min\{u_i \pmod{m_{i+1}}, m_{i+1} - u_i \pmod{m_{i+1}}\}.$$

5. If $m_{i+1} = 1$, then go to step 6 (in this case equation holds $m_i = u_i^2 + 1^2 \cdot 2$), else $i \leftarrow i + 1$ and go to step 4.
6. $a_i \leftarrow u_i$, $b_i \leftarrow 1$.
7. If $i = 0$, then $a \leftarrow a_i$, $b \leftarrow b_i$ and go to step 9. Else

$$a_{i-1} \leftarrow \frac{\pm u_{i-1}a_i + 2b_i}{a_i^2 + 2b_i^2},\ b_{i-1} \leftarrow \frac{-a_i \pm u_{i-1}b_i}{a_i^2 + 2b_i^2}.$$

   Signs are to be chosen so that division result is integer.
8. Set $i \leftarrow i - 1$ and go to step 7.
9. Return: a, b. **n**

This algorithm can be applied to real quadratic order $\mathbb{Z}[\sqrt{2}]$, which differs from imaginary order by infinite group of units. In practice it is never mind which of numbers r, $-r$ is represented as $a^2 - 2b^2$. If $r = a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2})$, then $-r = 2b^2 - a^2 = (a + b\sqrt{2})(1 + \sqrt{2})(a - b\sqrt{2})(1 - \sqrt{2})$. So more convenient representation can be obtained by multiplication of divisor $a + b\sqrt{2}$ by unit $1 \pm \sqrt{2}$ with norm –1.

For factoring prime number in $\mathbb{Z}[\sqrt[4]{-2}]$ firstly factor r in ring $\mathbb{Z}[\sqrt{-2}]$:

$$r = (a + b\sqrt{-2})(a - b\sqrt{-2}) = \pi\bar{\pi} = a^2 + 2b^2, \qquad (2)$$

where $a + b\sqrt{-2} \equiv 0 \pmod{r}$, and then find factorization of this prime quadratic number in ring $\mathbb{Z}[\sqrt[4]{-2}]$:

$$a + b\sqrt{-2} = (c + d\sqrt[4]{-2} + e\sqrt[4]{-2}^2 + f\sqrt[4]{-2}^3)(c - d\sqrt[4]{-2} + e\sqrt[4]{-2}^2 - f\sqrt[4]{-2}^3) = \rho\bar{\rho}. \qquad (3)$$

Prime quadratic number $\pi = a + b\sqrt{-2}$ defines finite field $\mathbb{Z}[\sqrt{-2}]/(\pi)$ of r elements. This field consists of residue classes modulo π — quadratic integers τ, which norm $N(\tau) = \tau\bar{\tau}$ satisfies inequality $N(\tau) \le N(\tau + \beta\pi)$ for any $\beta \in \mathbb{Z}[\sqrt{-2}]$. Since norm of imaginary quadratic integer is non-negative, such τ always exists.

To compute such τ define quadratic integer $\beta = n_0 + n_1\sqrt{-2}$, that norm $N(\tau + \beta\pi)$ is minimal. Norm $N(\tau + \beta\pi)$ is quadratic function of n_0, n_1. Optimal integers n_0, n_1 can be defined by computing derivations of norm $N(\tau + \beta\pi)$ by variables n_0, n_1 and finding the nearest integers.

Algorithm 2. Computing field isomorphism $\mathbb{F}_r \to \mathbb{Z}[\sqrt{-2}]/(\pi)$.

Input: $k \in \mathbb{F}_r$, r, $\pi = a + b\sqrt{-2}$.

Output: $k_0 + k_1\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]/(\pi)$.

Method.

1. Set $k_0 \leftarrow k$, $k_1 \leftarrow 0$.
2. Until $n_0 \neq 0$, $n_1 \neq 0$, do

a. Find: $n_0 = \left[\frac{ak_0 + 2bk_1}{r} \right]$ and set $k_0 + k_1\sqrt{-2} \leftarrow k_0 + k_1\sqrt{-2} - n_0\pi$.

b. Find: $n_1 = \left[\frac{ak_1 - bk_0}{r} \right]$ and set $k_0 + k_1\sqrt{-2} \leftarrow k_0 + k_1\sqrt{-2} - n_1\pi\sqrt{-2}$.

3. Return: k_0, k_1. **n**

Algorithm 2 determines reduction in ring $\mathbb{Z}[\sqrt{-2}]$ modulo prime ideal (π) and hence determines isomorphism of finite fields $\mathbb{F}_r \to \mathbb{Z}[\sqrt{-2}]/(\pi)$. Now one can apply algorithm 1 to find factorization (3) of quadratic prime integer π in ring $\mathbb{Z}[\sqrt[4]{-2}]$. In this case all computation is performed in ring $\mathbb{Z}[\sqrt{-2}]$, and in corresponding formulas integer 2 is to be changed by quadratic integer $\sqrt{-2}$.

According to (2) number $\pi = a + b\sqrt{-2}$ is determined up to sign, hence, any one of integers π, $-\pi$ can be factored. General length of coefficients of number ρ must be minimal. To minimize the general length obtained prime algebraic number ρ can be multiplied by a unit of ring $\mathbb{Z}[\sqrt[4]{-2}]$. Notice that number ρ can be defined once, when cryptosystem parameters are computed.

Similarly prime factorization of group order can be determined in ring $\mathbb{Z}[\sqrt[4]{2}]$. Since the quadratic integer norm can be negative, in algorithm 2 absolute norm must be minimized.

According to quadratic reciprocity low prime r can be factored in $\mathbb{Z}[\sqrt{-2}]$ and in $\mathbb{Z}[\sqrt[4]{-2}]$ if $r \equiv 3 \pmod 8$. Similarly prime r can be factored in $\mathbb{Z}[\sqrt{2}]$ and in $\mathbb{Z}[\sqrt[4]{2}]$ if $r \equiv 7 \pmod 8$.

3. Fast exponentiation method

Consider fast exponentiation methods for the fixed element of cyclic group. Few variants are possible: using rings $\mathbb{Z}[\sqrt{\pm 2}]$ or $\mathbb{Z}[\sqrt[4]{\pm 2}]$, using window size 2 or 4 bits. In dependence of ring used the number of doublings can be reduced 2 or 4 times with respect to usual binary exponent representation and the same window size. For example, if ring $\mathbb{Z}[\sqrt[4]{-2}]$ is used, four bit window corresponds to elements $\sum_{i=0}^{3} e_i \sqrt[4]{-2}^i P$, $e_i \in \{-1, 0, 1\}$. Since we raise the fixed element of cyclic group, then all such elements can be stored in computer memory. Transition to next window takes only one doubling. Two bit window corresponds to elements $e_0 P + e_1 \sqrt[4]{-2} P$. If cyclic group is elliptic curve with $j = 20^3$, then transition to next window takes only one complex multiplication by $\sqrt{-2}$.

If quadratic order $\mathbb{Z}[\sqrt{\pm 2}]$ and finite field $\mathbb{F}_r \cong \mathbb{Z}[\sqrt{\pm 2}]/(\pi)$ is used, any exponent $0 < k < r$ can be represented as $k \equiv k_0 + k_1\sqrt{\pm 2} \pmod{\pi}$ by algorithms 1 and 2 so that its absolute norm is minimal. Total length of k_0, k_1 is less or equal to length of r.

Let prime divisor $\rho \in \mathbb{Z}[\sqrt[4]{-2}]$ of the group order r with minimal norm over $\mathbb{Z}$ is computed. Then any exponent $0 < k < r$ can be represented as set (k_0, k_1, k_2, k_3): $k \equiv \sum_{i=0}^{3} k_i \sqrt[4]{-2}^i \pmod{\rho}$ so that norm of this algebraic integer is minimal. Find algebraic integer $\beta = \sum_{i=0}^{3} n_i \sqrt[4]{-2}^i$ so that norm $N(k - \beta\rho)$ in $\mathbb{Z}$ is minimal. For this firstly find approximation to k in quadratic order $\mathbb{Z}[\sqrt{-2}]$ using algorithm 2, then apply algorithm 2 to extension $\mathbb{Z}[\sqrt[4]{-2}]/\mathbb{Z}[\sqrt{-2}]$. Derivation of norm function is linear function of n_i, what simplifies computation (directly norm $\mathbb{Q}[\sqrt[4]{-2}]/\mathbb{Q}$ computation leads to solving cubic equations, this will complicate finding of n_i).

Algorithm 3. Computing field isomorphisms $\mathbb{Z}[\sqrt[4]{-2}]/(\rho)$ and $\mathbb{Z}[\sqrt{-2}]/(\pi)$.

Input: $k_0 + k_2\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]/(\pi)$, π, $\rho = c + d\sqrt[4]{-2} + e\sqrt[4]{-2}^2 + f\sqrt[4]{-2}^3$.

Output: $k_0 + k_1\sqrt[4]{-2} + k_2\sqrt[4]{-2}^2 + k_3\sqrt[4]{-2}^3 \in \mathbb{Z}[\sqrt[4]{-2}]/(\rho)$.

Method.

1. Set $k_1 \leftarrow 0$, $k_3 \leftarrow 0$, $\kappa = k_0 + k_1\sqrt[4]{-2} + k_2\sqrt[4]{-2}^2 + k_3\sqrt[4]{-2}^3$.
2. While n_0, n_1, n_2, $n_3 \neq 0$, find integers n_i that give minimal norm in $\mathbb{Z}$ of $\kappa - n_i\rho\sqrt[4]{-2}^i$ and set $\kappa \leftarrow \kappa - n_i\rho\sqrt[4]{-2}^i$.
3. Return: $\kappa = k_0 + k_1\sqrt[4]{-2} + k_2\sqrt[4]{-2}^2 + k_3\sqrt[4]{-2}^3 \in \mathbb{Z}[\sqrt[4]{-2}]/(\rho)$. **n**

Consider variants of exponentiation algorithm. Let ring $\mathbb{Z}[\sqrt{-2}]$ is used (–2 is quadratic residue modulo r). Find factorization (2) using algorithm 1 and find representation $k \equiv k_0 + k_1\sqrt{-2} \pmod{\pi}$ using algorithm 2: $k_0 = k_{00} + 2k_{01} + 2^2k_{02} + \ldots$, $k_1 = k_{10} + 2k_{11} + 2^2k_{12} + \ldots$ Write exponent k in number system with base $\sqrt{-2}$:

$$k \equiv k_{00} + k_{10}\sqrt{-2} - k_{01}\sqrt{-2}^2 - k_{11}\sqrt{-2}^3 + \ldots \pmod{\pi}.$$

If signs of integers k_0, k_1 are the same, then signs alternation is +, +, –, –, +, +, –, – or its inverse. This is normal alternation signs. If signs of k_0, k_1 are different, then alternation of signs is not normal (+, –, –, + or its inverse). Sometimes it is sufficient to use precomputation base only for normal alternation of signs, i.e. $\{e_0P + e_1\sqrt{-2}P - 2e_2P - 2e_3\sqrt{-2}P\}$, $e_i \in \{0, 1\}$. For example, if elliptic curve has complex multiplication by $\sqrt{-2}$, normal alternation of signs can be obtained by exponent representation as

$$k \equiv k_{00} + \sqrt{-2}(k_{10} - k_{01}\sqrt{-2} - k_{11}\sqrt{-2}^2 + \ldots) \pmod{\pi}. \quad (4)$$

Number in brackets has normal alternation of signs. Assume that we can multiply elliptic curve point by an exponent with normal alternation of signs. Then we

can multiply it by an exponent with arbitrary alternation: firstly multiply point by an exponent in brackets (4), apply complex multiplication and add point $k_{00}P$.

If real quadratic ring $\mathbb{Z}[\sqrt{2}]$ is used and factorization of group order is $\pm r = \pi\bar{\pi} = a^2 - 2b^2$, normal alternation of signs corresponds to the same signs of k_0, k_1. To obtain normal alternation of signs it is necessary to transform in (4) $k \leftarrow k \pm u^{\varepsilon}\pi$, where u is fundamental unit and $\varepsilon \in \{-1, 0, 1\}$.

Both in imaginary and real quadratic rings transition to next number takes two doublings for 4 bit window and one doubling for 2 bit window.

Let ring $\mathbb{Z}[\sqrt[4]{-2}]$ is used and prime divisor $\rho \in \mathbb{Z}[\sqrt[4]{-2}]$ of group order is known. For multiply point P by integer k, find algebraic representation of k: $k_0 + k_1\sqrt[4]{-2} + k_2\sqrt[4]{-2}^2 + k_3\sqrt[4]{-2}^3 \in \mathbb{Z}[\sqrt[4]{-2}]/(\rho)$. Let $k_i = k_{i0} + 2k_{i1} + \ldots$ — binary digits of its coefficients. Write exponent k in number system with base $\sqrt[4]{-2}$:

$$k = k_{00} + k_{10}\sqrt[4]{-2} + k_{20}\sqrt[4]{-2}^2 + k_{30}\sqrt[4]{-2}^3 - k_{01}\sqrt[4]{-2}^4 - \ldots \qquad (5)$$

Define normal alternation of signs: +, +, +, +, –, –, –, – or its inverse. This corresponds to the case when all k_i has the same sign. Normal alternation can by obtained by changing in (5): $k \leftarrow k \pm \beta\rho$, where $\beta \in \mathbb{Z}[\sqrt[4]{-2}]$ is "small" algebraic integer (with small absolute norm). Precomputation table contains 15 or 3 elements for window size 4 or 2 bits respectively.

If window size is 4 bits, then transmitting to next window takes only one point doubling. If window size is 2 bits, then transmitting to next window takes only one complex multiplication by $\sqrt{-2}$.

For ring $\mathbb{Z}[\sqrt[4]{2}]$ exponentiation method is performed similarly. But exponent representation takes considering two generators of group of units, so exponent representing as element of ring $\mathbb{Z}[\sqrt[4]{2}]$ with minimal length is less convenient. This reasoning shows that use of rings $\mathbb{Z}[\sqrt[8]{\pm 2}]$ may have little or no advantage since rank of its group of units increases.

Consider the complexity of elliptic curve point multiplication if length of exponent is N bits and window size is 4 bits. Usual method takes $12\frac{N}{4} + 13N$ modular multiplications. If ring $\mathbb{Z}[\sqrt{\pm 2}]$ is used, point multiplication takes $12\frac{N}{4} + 13\frac{N}{2}$ modular multiplications. If ring $\mathbb{Z}[\sqrt[4]{\pm 2}]$ is used, point multiplication takes $12\frac{N}{4} + 13\frac{N}{4}$ modular multiplications. Hence, for $N = 160$ bits point exponentiation can be speeded-up about 1.6 times for quadratic ring and about 2.5 times for ring $\mathbb{Z}[\sqrt[4]{\pm 2}]$ comparatively to known methods. The hardest operation during digital signature verification according to ECDSA is elliptic curve fixed point multiplication. So proposed method allows speeding-up digital signature verification 1.6 or 2.5 times for window size 2 or 4 bits respectively.

Consider small numerical example for the rings $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt[4]{-2}]$. Let r = 64019. Find $\sqrt{-2} \equiv -5625 \pmod{r}$, $\sqrt[4]{-2} \equiv 9241 \pmod{r}$. Find prime algebraic divisors of prime integer r using algorithm 1:

$$\pi = 231 + 73\sqrt{-2}\,,\ \rho = -3 + 7\sqrt[4]{-2} + \sqrt[4]{-2}^2 + 8\sqrt[4]{-2}^3.$$

Let k = 12345. Find image of k in finite field $\mathbb{Z}[\sqrt{-2}]/(\pi)$. Algorithm 2 gives n_0 = 45, n_1 = –14 and exponent is $k \equiv -94 - 51\sqrt{-2} \pmod{\pi}$.

Find image of the exponent in finite field $\mathbb{Z}[\sqrt[4]{-2}]/(\rho)$:

$$-94 - 51\sqrt{-2} \equiv 0 + 0\sqrt[4]{-2} - 3\sqrt[4]{-2}^2 + 6\sqrt[4]{-2}^3 \pmod{\rho}.$$

Exponent k representation base $\sqrt[4]{-2}$ is

$$k \equiv -\sqrt[4]{-2}^2 + \sqrt[4]{-2}^6 + \sqrt[4]{-2}^7 - \sqrt[4]{-2}^{11} \pmod{\rho}.$$

If window size is 4 bits, then exponent k is given by quadriples –**(**0, 0, 1, 0**)**, **(**0, 0, 1, 1**)**, –**(**0, 0, 0, 1**) (**beginning from the least significant digits**)**. Alternation of signs is normal. The next window passage takes one doubling. So only two doublings and two additions are needed. If known method with the same window size is used, then 12345 = $3 \cdot 16^3 + 3 \cdot 16 + 9$. Exponentiation takes two additions and eight doublings.

References

1. J. Cohen. A course in computational algebraic number theory, Springer-Verlag, 1996.
2. FIPS 186, Digital Signature Standard, Federal Information Processing Standards Publication 186, U.S. Department of Commerce/ N.I.S.T., National Technical Information Service, Springfield, Virginia.
3. H.R. Frium. The group low on elliptic curves in Hesse form. Technical report corr2001-09.
4. D. Gordon. A survey of fast exponentiation methods // Journal of algorithms, 27 (1998), 129–146.
5. F. Lemmermeyer. The Euclidean algorithm in algebraic number fields, Expo. Math. 13, No. 5 (1995), 385-416.
6. A. Menezes, P. van Oorchot and S. Vanstone. Handbook of applied cryptography. — CRC Press, 1997.
7. J. Pollard and C. Schnorr. An effective solution of the congruence $x^2 + ky^2 = m \pmod{n}$ // IEEE proceedings on Information theory, v. 33 (1987), 702-709.
8. A.G. Rostovtsev and E.B. Makhovenko. Elliptic curve point multiplication // IACR e-print archive, 2003/088.