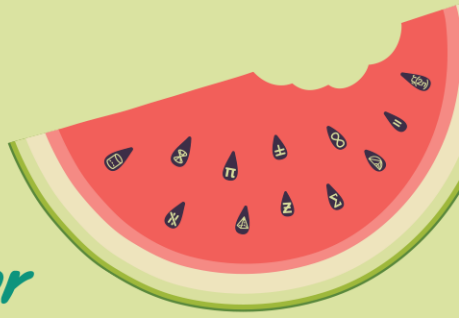
AMSI SUMMER RESEARCH SCHOLARSHIPS 2024–25

Get a taste for Research this Summer



Modular Algorithms for Computation in Quadratic Algebraic Extension Fields

Mitchell Holt

Supervised by Dr Paul Vrbik

The University of Queensland

Jane Street®

AMSI AUSTRALIAN MATHEMATICAL SCIENCES INSTITUTE

Abstract

In this report, we give a generalisation of the notion of modular algorithms to quadratic algebraic number fields. We show that there are infinitely many integer primes that we can use for fast and effective modular arithmetic in these fields, and give an algorithm to construct these primes. Finally, we show that we can use Garner's algorithm for Chinese remaindering in quadratic number fields and show that this allows us to use a well-known rational linear system solver over these fields.

Contents

1 Introduction

Computer algebra is the field of mathematics and computer science dedicated to designing algorithms for exact and symbolic computation. Unlike other fields of mathematics, in computer algebra we are interested in taking objects we know how to compute, and studying them with the motivation of finding faster, or more efficient algorithms to compute them.

However, the trade we make for exact computation is that exact algorithms are often slow and inefficient. A contributor to this is the problem of *expression swell*, where the intermediate expressions used during the execution of an algorithm are far larger than those that appear in the output.

One of the most successful strategies for addressing expression swell is the *modular algorithm*, which is an algorithm that computes something by reconstructing it from modular images. Modular algorithms over $\mathbb{Z}$ (and $\mathbb{Q}$) are well-understood, and have led to significant improvements in a variety of applications, including polynomial factorisation, linear system solving, and sparse multivariate polynomial interpolation.

Consider a *quadratic algebraic number field* $\mathbb{Q}(\sqrt{M})$, where M is any squarefree integer. Since $\mathbb{Q}(\sqrt{M})$ is a 2-dimensional $\mathbb{Q}$-algebra, expression swell in $\mathbb{Q}(\sqrt{M})$ is at least as bad as in $\mathbb{Q}$. In this report, we introduce modular algorithms over $\mathbb{Q}$, before giving results allowing us to generalise modular algorithms to $\mathbb{Q}(\sqrt{M})$. We conclude by giving an example of a modular algorithm in a quadratic number field.

2 Modular Algorithms

In this section, we briefly outline an important tool for modular algorithms over $\mathbb{Z}$ (or $\mathbb{Q}$), with the goal of presenting a fast and effective modular algorithm to solve linear systems.

Example 2.1 ([GCL92, §5.2])**.** Consider the system of linear equations

$$\begin{aligned} 22x + 44y + 74z &= 1, \\ 15x + 14y - 10z &= -2, \\ -25x - 28y + 20z &= 34. \end{aligned} \tag{1}$$

A natural approach to solve this in $\mathbb{Q}$ is to write it as a matrix equation and find a solution using Gaussian elimination on an augmented matrix. With fractions, we generally have two choices for representations: we can simplify at each step by dividing the numerator and the denominator by their greatest common divisor, giving smaller integers, or we can allow the numerators and denominators to grow arbitrarily large. Both of these options introduce an overhead cost to using fractions, so often algorithms in computer algebra will use a *fraction-free* method.

Using fraction-free Gaussian elimination, we reduce the system of equation (1) to the system

$$\begin{aligned} 1257315840x &= 7543895040, \\ -57150720y &= 314328960, \\ 162360z &= 243540, \end{aligned} \tag{2}$$

giving the solution $\{x = 6,\ y = -\frac{11}{2},\ z = \frac{3}{2}\}$.

Observe that the integers in equation (2) are much larger than the integers in the solution, a clear example of expression swell. It is not unexpected for the integers to be so large; Cramer's rule (Theorem 2.2) tells us that each rational in the solution is a ratio of two determinants. Moreover, the size of the integers used in fraction-free Gaussian elimination grow linearly as the algorithm runs, so we expect to be performing arithmetic with large integers for a non-trivial portion of the runtime. ■

2.1 The Chinese Remainder Theorem

The Chinese remainder theorem is one of the most important theorems for modular algorithms, allowing us to recover an integer result from several modular images.

Theorem 2.1 (Chinese Remainder Theorem)**.** *Let $m_0, \ldots, m_n \in \mathbb{Z}$ be pairwise coprime and let $u_0, \ldots, u_n \in \mathbb{Z}$ be any integers. There exists a $u \in \mathbb{Z}$, unique modulo $m_0 \cdots m_n$, such that $u \equiv u_i \pmod{m_i}$, $i = 0, \ldots, n$.*

Proof. Consider the homomorphism

$$\phi : \mathbb{Z} \to (\mathbb{Z}/m_0\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z}),$$
$$\phi(u) = (u \pmod{m_0}, \ \ldots, \ u \pmod{m_n}).$$

Let us begin by showing that $\ker\phi = \langle \operatorname{lcm}(m_0, \ldots, m_n)\rangle$. First, suppose that $k \in \ker\phi$. Then $k \equiv 0 \pmod{m_i}$ for all $i = 0, \ldots, n$; in particular, k is divisible by $\operatorname{lcm}(m_0, \ldots, m_n)$, and hence $k \in \langle \operatorname{lcm}(m_0, \ldots, m_n)\rangle$. On the other hand, if $k \in \langle \operatorname{lcm}(m_0, \ldots, m_n)\rangle$, then certainly $k \equiv 0 \pmod{m_i}$ for all $i = 0, \ldots, n$, and hence $k \in \ker\phi$.

Now, since the m_i are coprime, $\ker\phi = \langle \operatorname{lcm}(m_0, \ldots, m_n)\rangle = \langle m_0 \ldots m_n\rangle$. It follows that there is an injection $\psi : (\mathbb{Z}/m_0 \cdots m_n\mathbb{Z}) \to (\mathbb{Z}/m_0\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$. As ψ is an injection between finite sets of the same cardinality, it is also a surjection. The surjectivity of ψ implies a solution exists, and injectivity uniqueness of the solution modulo $m_0 \cdots m_n$. □

Of course, this proof does not give us any hints as to how we might efficiently compute such a u. Garner [Gar59] gives an algorithm to produce the smallest solution by constructing the coefficients $v_0, \ldots, v_n$ of the *mixed-radix* representation

$$u = v_0 + v_1(m_0) + v_2(m_0m_1) + \cdots + v_n \prod_{i=0}^{n-1} m_i, \tag{3}$$

building it one modulus at a time. We present an algorithm to construct the mixed-radix coefficients in a more general ring in §4, accompanied by a proof of correctness.

2.2 A Modular Linear Solver

So that we can demonstrate that the generalisation of modular algorithms to quadratic number fields gives the same increases in efficiency that we would expect, we give the example of a modular algorithm that solves linear systems - here over the rationals, and in §4 over a quadratic number field. The modular linear solver (Algorithm 2.1) we present was discovered independently by [TI61] and [CL77], and uses Chinese remaindering. We note that there are faster and more effective algorithms that use other methods (such as [Dix82], which uses p-adic lifting and rational reconstruction), but for our purposes it is a little easier to look at the earlier algorithm.

For Algorithm 2.1 and the accompanying proof of correctness (Proposition 2.1), we use the notation $A_{i|b}$ to denote the matrix formed from A by replacing the i-th column of A with the vector b.

Proposition 2.1. *Algorithm 2.1 is correct.*

For this proof, we use a well-known result from linear algebra first due to [Cra50], omitting the proof.

Algorithm 2.1 Linear Solver [TI61],[CL77]

Input: A a non-singular $n \times n$ matrix with integer entries, and b any $1 \times n$ column vector with integer entries.

Output: A vector x with rational entries satisfying $Ax = b$.

1: $p_1, \ldots, p_k \leftarrow$ distinct primes with $\prod_{i=1}^{k} p_i > 2\max(|\det A|, |\det A_{1|b}|, |\det A_{2|b}|, \ldots, |\det A_{n|b}|)$

2: **for** $i = 1, \ldots, n$ **do**

3: $\quad d_i \leftarrow \det A \pmod{p_i}$

4: $\quad x_i \leftarrow$ solve $Ax = b \pmod{p_i}$

5: **end for**

6: $D \leftarrow$ Chinese remainder theorem on $\{d_1 \pmod{p_1}, \ldots, d_n \pmod{p_n}\}$

7: $y \leftarrow$ pointwise Chinese remainder theorem on $\{d_1 \cdot x_1 \pmod{p_1}, \ldots, d_n \cdot x_n \pmod{p_n}\}$

8: **return** $1D \cdot y$

Theorem 2.2 (Cramer's Rule)**.** *Let R be an integral domain with field of fractions F, $A \in R^{n\times n}$ non-singular, and $b \in R^n$ any vector. The entries of the solution vector $x \in F^n$ to $Ax = b$ are given by*

$$x_i = \frac{\det A_{i|b}}{\det A}, \qquad i = 1, \ldots, n. \tag{4}$$

Proof (of Proposition 2.1). Let $m = p_1 \cdots p_k$. The Chinese Remainder theorem (Theorem 2.1) gives us unique solutions D, y modulo m, and we of course take those solutions in $\mathbb{Z}$ for $D, y_1, y_2, \ldots, y_n$ with the *smallest absolute value*.

Since $m > 2|\det A| = (0 + |\det A|) - (0 - |\det A|)$, D is certainly either $-|\det A|$ or $|\det A|$; that is, $D = \det A$ is the solution with the correct sign. We can use the same argument to see that, for each i with $1 \le i \le n$, $y_i = D \cdot \det A_{i|b}$. Cramer's rule (Theorem 2.2) then gives us that $x_i = y_i/D$ as desired. □

Example 2.2. Returning to Example 2.1, we observe that running Algorithm 2.1 gives the same (correct) solution. However, while fraction-free Gaussian elimination uses integers as large as 32 bits on this example, the modular solver reconstructs integers that are only 15 bits! ■

3 Quadratic Number Fields, Algebraic Integers, and Primes

Let M be squarefree and consider the *quadratic algebraic number field* $\mathbb{Q}(\sqrt{M})$. This field is the smallest containing all of $\mathbb{Q}$ and $\sqrt{M}$, and can be explicitly constructed as the quotient $\mathbb{Q}[x]/\langle x^2 - M\rangle$ of the polynomial ring with coefficients in $\mathbb{Q}$. Since we are interested in generalising the notion of modular algorithms to these fields, we need to consider what it means to be prime, and to do modular arithmetic. A precursor to both of these concepts is the idea of the *ring of algebraic integers*, which generalises the relationship that the integers have to the rationals.

3.1 Quadratic Integers

Definition 3.1 (Algebraic Integers)**.** The *algebraic integers* of an algebraic extension K of $\mathbb{Q}$ are the elements of K that are the roots of polynomials with coefficients in $\mathbb{Z}$.

For the purposes of this report, we are only interested in the algebraic integers of the quadratic number fields $\mathbb{Q}(\sqrt{M})$, which we call the *quadratic integers*. We show in Theorem 3.1 that we can write the form of any quadratic integer explicitly, and an immediate consequence of this is that the quadratic integers form a ring. Since [Mar77] does not prove the theorem, we will do it here.

Theorem 3.1 ([Mar77, Corollary 2 to Theorem 1])**.** *Let $M \in \mathbb{Z}$ be squarefree. The quadratic integers (of $\mathbb{Q}(\sqrt{M})$) are $R = \mathbb{Z}[\gamma]$, where*

$$\gamma = \begin{cases} \sqrt{M} & M \equiv 2 \pmod 4 \text{ or } M \equiv 3 \pmod 4, \\ \dfrac{1+\sqrt{M}}{2} & M \equiv 1 \pmod 4. \end{cases}$$

Proof. Suppose that $\alpha = r + s\sqrt{M}$ is a quadratic integer. Then it is the root of some monic irreducible polynomial with coefficients in $\mathbb{Z}$. Indeed, the monic irreducible polynomial over $\mathbb{Q}$ having α as a root has coefficients in $\mathbb{Z}$ [Mar77, Theorem 1].

If $s = 0$, then α is a root of $x - r$, implying that $r \in \mathbb{Z}$. The result follows immediately in this case. Otherwise, the minimal polynomial of α in $\mathbb{Q}[x]$ (and hence $\mathbb{Z}[x]$) is

$$f := x^2 - 2rx + r^2 - Ms^2 \tag{5}$$

Thus α is an algebraic integer if and only if both $2r$ and $r^2 - Ms^2$ are integers. From here, we show that:

(i) $\mathbb{Z}[\sqrt{M}] \subseteq \mathbb{Z}[\frac{1+\sqrt{M}}{2}]$.

(ii) Every quadratic integer is contained in $\mathbb{Z}[\frac{1+\sqrt{M}}{2}]$.

(iii) If $\alpha \in \mathbb{Z}[\frac{1+\sqrt{M}}{2}] \setminus \mathbb{Z}[\sqrt{M}]$, then $M \equiv 1 \pmod 4$.

For (i), we simply notice that any element $a + b\sqrt{M} \in \mathbb{Z}[\sqrt{M}]$ can be written as $(a-b) + 2b(\frac{1+\sqrt{M}}{2}) \in \mathbb{Z}[\frac{1+\sqrt{M}}{2}]$. We show (ii) and (iii) in two cases, depending on the parity of $2r$ (the coefficient of x in the minimal polynomial of α equation (5)).

Case 1. Suppose that $2r$ is even; that is, $r \in \mathbb{Z}$. Then $r^2 - Ms^2 \in \mathbb{Z}$ if and only if $Ms^2 \in \mathbb{Z}$. Write $s = \frac{p}{q}$, where $q > 0$ and $\gcd(p, q) = 1$. It follows that $Ms^2 = \frac{Mp^2}{q^2}$ is an integer if and only if $q^2 \mid Mp^2$. Since α is assumed to be an algebraic integer, we must have $q^2 \mid Mp^2$, so $\gcd(p, q) = 1 \implies \gcd(p^2, q^2) = 1 \implies q^2 \mid M$ But M is squarefree, so we have $q^2 = 1 \implies q = 1$ (since $q > 0$). Thus $s = \frac{p}{1} \in \mathbb{Z}$. Therefore $\alpha \in \mathbb{Z}[\sqrt{M}]$, so both (ii) and (iii) hold.

Case 2. Suppose that $2r$ is odd; that is, $2r = 2j + 1$ for some $j \in \mathbb{Z}$. Then the constant coefficient of the minimal polynomial equation (5) is

$$r^2 - Ms^2 = \frac{4j^2 + 4j + 1 - 4Ms^2}{4} = j^2 + j + \frac{1 - 4Ms^2}{4} \tag{6}$$

Let $s = \frac{p}{q}$, where $q > 0$ and $\gcd(p, q) = 1$. We see that

$$\begin{aligned} r^2 - Ms^2 \in \mathbb{Z} &\iff \frac{1 - 4Ms^2}{4} \in \mathbb{Z} && \text{(by equation (6))} \\ &\iff 4Ms^2 \equiv 1 \pmod 4 \\ &\iff 4Mp^2 \equiv q^2 \pmod 4 \\ &\iff q^2 \equiv 0 \pmod 4 \\ &\iff q \equiv 0 \pmod 2 \end{aligned}$$

So $q = 2n$ for some $n \in \mathbb{Z}$, $n > 0$. As p, q are coprime, this implies that p is odd, so $p = 2k + 1$ for some $k \in \mathbb{Z}$. Then:

$$\begin{aligned} \frac{1 - 4Ms^2}{4} \in \mathbb{Z} &\iff \frac{1 - \frac{4Mp^2}{4n^2}}{4} \in \mathbb{Z} \\ &\iff \frac{1 - \frac{Mp^2}{n^2}}{4} \in \mathbb{Z} \\ &\iff \frac{Mp^2}{n^2} \equiv 1 \pmod 4 \end{aligned}$$

Now, as $1 = \gcd(p, q) = \gcd(p^2, q^2) = \gcd(p^2, 2n^2)$, we have $n^2 \mid Mp^2 \implies n^2 \mid M$. Since M is squarefree, we must have $n^2 = 1$, which implies that $n = 1$ (as $n > 0$). Thus

$$1 \equiv Mp^2 \equiv M(2k + 1)^2 \equiv 4k^2M + 4kM + M \equiv M \pmod 4$$

Hence $\alpha \in \mathbb{Z}[\frac{1+\sqrt{M}}{2}] \setminus \mathbb{Z}[\sqrt{M}]$ in this case and $M \equiv 1 \pmod 4$ necessarily, so we have (ii) and (iii). □

Now we turn to consider the primes of the quadratic integers. We often want to be able to work over a field when working modulo a prime, so we are especially interested in the prime ideals that are also maximal. Fortunately, the quadratic integers have Krull dimension 1; that is, all the non-zero prime ideals are maximal [Mar77, Theorem 14]. Unfortunately, the quadratic integers are not a principle ideal domain. It is generally accepted that computation is much more expensive when we are working modulo an ideal with more than one generator, and things as seemingly simple as checking equality become non-trivial.

We therefore restrict our attention to the prime ideals that are generated by a single quadratic integer. Of course, it is computationally most efficient if that generator is an integer prime. We call any integer prime that is also prime in a ring of quadratic integers R an *inert* prime of R. Miraculously, there are infinitely many inert primes in every ring of quadratic integers. The remainder of this section is dedicated to characterising and computing inert primes in arbitrary rings of quadratic integers. Many of the results stated or proved are

restrictions of more general results from algebraic number theory to the case where we are considering the algebraic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$.

For the remainder of the section, we fix $M \in \mathbb{Z}$ a squarefree integer, and let R be the ring of integers of $\mathbb{Q}(\sqrt{M})$.

Definition 3.2 (Ramification Index and Inertial Degree)**.** Let $p \in \mathbb{Z}$ be a prime. For each prime ideal Q dividing pR, define:

(i) The *ramification index* of Q, denoted $e(Q|p)$, is the largest positive integer e such that $Q^e \mid pR$.

(ii) The *inertial degree* of Q, denoted $f(Q|p)$, is the index of $\mathbb{Z}/p\mathbb{Z}$ in R/Q.

Theorem 3.2 (Special case of [Mar77, Theorem 21])**.** *Let $p \in \mathbb{Z}$ be prime, and $Q_1, \ldots, Q_r$ be the prime ideals of R dividing pR. Then*

$$\sum_{i=1}^{r} e(Q_i|p) f(Q_i|p) = 2$$

The splitting of integer primes in $\mathbb{Q}(\sqrt{M})$ is described by [Mar77, Theorem 25]. However, we are only interested in a special case of this theorem, and as the reference does not provide a full proof of the result, we will give one here.

Theorem 3.3 (Special case of [Mar77, Theorem 25])**.** *Let $p \in \mathbb{Z}$ be a prime not dividing M. Then p is inert in R if and only if there is no $n \in \mathbb{Z}$ with $M \equiv n^2 \pmod{p}$.*

Before we can prove the theorem, we consider some necessary results giving us a sufficient condition for a prime to be inert, and a useful property of the bases for a class of ideals we are interested in, respectively.

Lemma 3.1. *Let $p \in \mathbb{Z}$ be prime, and Q be any prime of R dividing pR. If R/Q and $\mathbb{Z}/p\mathbb{Z}$ are not isomorphic, then pR is prime.*

Proof. Suppose that $R/Q \not\cong \mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ is the unique finite field of order p (up to isomorphism), we see that the index $[R/Q : \mathbb{Z}/p\mathbb{Z}] \neq 1$. It follows from Theorem 3.2 that $2 = [R/Q : \mathbb{Z}/p\mathbb{Z}] = f(Q|p)$, so $e(Q|p) = 1$ and Q is in fact the only prime of R dividing pR. Thus, $pR = Q$ which is prime. □

Lemma 3.2. *Suppose that $p \nmid M$ and $n^2 - M \equiv 0 \pmod{p}$ for some $M, n \in \mathbb{Z}$, and odd prime $p \in \mathbb{Z}$. Then there exists a $k \in \mathbb{Z}$ such that $k^2 - M \equiv 0 \pmod{p}$, but $k^2 - M \not\equiv 0 \pmod{p^2}$.*

Proof. If $M - n^2 \not\equiv 0 \pmod{p^2}$, then we are done. Otherwise, we have

$$(n+p)^2 - M \equiv n^2 + 2np + p^2 - M \equiv 2np \pmod{p^2}$$

Since p is odd, $p \nmid 2$. We also know that $p \nmid n$. As p is prime, we have that $p \nmid 2n$, whence we conclude that $p^2 \nmid 2np$. Therefore, $k = n + p$ satisfies the proposition in this case. □

Proof (of Theorem 3.3). Let $p \in \mathbb{Z}$ be an odd prime not dividing M. First suppose that there is no integer $n \in \mathbb{Z}$ with $M \equiv n^2 \pmod{p}$ and consider the polynomial $h := x^2 - M$. As h has a root in $\mathbb{Q}(\sqrt{M})$ and has coefficients in $\mathbb{Z} \subset R$, h has a root in R. It follows that $h \pmod{pR}$ has a root in R/pR. However, h has no root in $\mathbb{Z}/p\mathbb{Z}$ by assumption. Therefore $\mathbb{Z}/p\mathbb{Z}$ and R/pR are not isomorphic, so by appealing to Lemma 3.1 we see that pR is prime.

Now suppose that there exists an $n \in \mathbb{Z}$ with $M \equiv n^2 \pmod{p}$. By Lemma 3.2, we may assume without loss of generality that $n^2 \not\equiv M \pmod{p^2}$. Let $I = \left\langle p, n + \sqrt{M} \right\rangle \left\langle p, n - \sqrt{M} \right\rangle$. To show that pR is not prime, we show that $pR = I$. Observe that $I = \left\langle p^2, p(n + \sqrt{M}), rp(n - \sqrt{M}), n^2 - M \right\rangle$. By assumption, $p \mid n^2 - M$, so we see that each generator of I is divisible by p. Therefore $I \subseteq \langle p \rangle$. On the other hand, I must contain the (integer) greatest common divisor $\gcd(p^2, n^2 - M) = p$, whence we have $\langle p \rangle \subseteq I$. This completes the proof. □

Recall that R/pR is a field if $p \in \mathbb{Z}$ is an inert prime. Although addition, subtraction, and multiplication in R/pR work in exactly the way we would expect, there is no immediately obvious algorithm to do (field) division. We complete our discussion of quadratic integers by characterising arithmetic in R/pR using an explicit isomorphism into a ring in which we can already perform fast arithmetic automatically. The isomorphism given is completely trivial to compute, reducing runtime overhead on a real computer. As the proof is a straight-forward application of the definitions, we omit it.

Proposition 3.1. *Let $p \in \mathbb{Z}$ be an inert prime in $R = \mathbb{Z}[\gamma]$ (where γ is as given in Theorem 3.1). Then*

$$R/pR \simeq \begin{cases} (\mathbb{Z}/p\mathbb{Z})[x]/\left\langle x^2 - M \right\rangle & M \equiv 2 \text{ or } 3 \pmod{4} \\ (\mathbb{Z}/p\mathbb{Z})[x]/\left\langle x^2 - x - \frac{M-1}{4} \right\rangle & M \equiv 1 \pmod{4} \end{cases}$$

with the isomorphism given by $\phi([a + b\gamma]) = [a + bx]$ in each case.

3.2 The Inert Prime Algorithm

For modular algorithms, we often want to work modulo several different primes. If there are only finitely many inert primes, modular algorithms may fail when the integers of the result are too large. Incredibly, there are infinitely many inert primes in *every* quadratic field! By Theorem 3.3, this is equivalent to showing that there are infinitely many primes p so that M is *not* a square modulo p. We present an algorithm (Algorithm 3.1) that computes inert primes. The existence of infinitely many primes is a corollary to the correctness of the algorithm, which we will prove after covering some necessary prerequisites from number theory.

Before we can prove the correctness of Algorithm 3.1, it is necessary to briefly introduce the theory of *quadratic residues*.

Definition 3.3. Let $p \in \mathbb{Z}$ be prime. We say that an integer $n \in \mathbb{N}$ is a *quadratic residue modulo p* if there exists a $k \in \mathbb{Z}$ with $n \equiv k^2 \pmod{p}$. If no such n exists, we say that n is a *quadratic non-residue modulo p*.

Algorithm 3.1 Inert primes

Input:

- Squarefree $M \in \mathbb{Z}$ with (distinct) prime factorisation $2^e q_1 q_2 \cdots q_n$, (e is 0 or 1).
- A finite set $\{\ell_1, \ell_2, \ldots, \ell_k\}$ of odd primes, not containing any of the q_i.
- If $M \neq 2$, an integer s which is a quadratic non-residue mod q_n

Output: A non-empty set S of primes, not containing any ℓ_i, for each of which M is a quadratic non-residue.

1: **if** $M = 2$ **then**

2: $\quad r \leftarrow \prod_{\substack{1 \le i \le k \\ \ell_i \neq 3}} \ell_i.$

3: $\quad b \leftarrow 8r + 3$

4: **else**

5: $\quad b \leftarrow$ Chinese remainder theorem on

$$\begin{aligned} x &\equiv 1 \pmod 8 \\ x &\equiv 1 \pmod{\ell_i}, \quad i = 1, \ldots, k \\ x &\equiv 1 \pmod{q_i}, \quad i = 1, \ldots, n-1 \\ x &\equiv s \pmod{q_n} \end{aligned}$$

6: **end if**

7: $P \leftarrow$ set of prime factors of b

8: **return** $\{p \in P \mid M^{(p-1)/2} \equiv -1 \pmod p\}$

Due to a result from Euler, we can easily test if an element $k \in \mathbb{Z}/p\mathbb{Z}$ (where p is prime) is a quadratic residue modulo p.

Theorem 3.4 (Euler's Criterion)**.** *Let p be an odd prime and let $a \in \mathbb{Z}$ be coprime to p. Then*

$$a^{(p-1)/2} \equiv \begin{cases} 1 \pmod p & a \text{ is a quadratic residue mod } p \\ -1 \pmod p & \text{otherwise} \end{cases}$$

Proof. This is a very well-known result. For example, [IR13, Proposition 5.1.2] gives a proof. □

Of course, we need to ensure that an input s to Algorithm 3.1 always exists. Once we have shown this, we can simply use Euler's Criterion (Theorem 3.4) to compute such an s.

Lemma 3.3. *Let $p > 2$ be prime. There exists an $s \in \mathbb{Z}$ that is a quadratic non-residue modulo p.*

Proof. Consider the endomorphism $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined $\phi(x) = x^2$. As $p > 2$, we have that $1 \neq -1$. But $\phi(1) = \phi(-1) = 1$, so ϕ is not injective. Now, ϕ is a mapping between finite sets of the same cardinality, so ϕ not injective implies that ϕ is not surjective. Therefore, we can take $s \in \mathbb{Z}/p\mathbb{Z} - \operatorname{im}\phi$ to prove the lemma. □

Using Euler's Criterion (Theorem 3.4), we obtain a nice algebraic definition of the *Legendre* and *Jacobi symbols*, and one can see that they are indeed homomorphisms.

Definition 3.4. Let $p \in \mathbb{Z}$ be an odd prime. The *Legendre symbol* is the homomorphism $\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ computing

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}$$

Definition 3.5. Let $b \in \mathbb{Z}$ be an odd, positive integer. Write $b = p_1 \cdots p_m$, where the p_i are (not necessarily distinct) odd primes. The *Jacobi symbol* is the homomorphism $\left(\frac{\cdot}{b}\right) : (\mathbb{Z}/b\mathbb{Z})^* \to \{\pm 1\}$ computing

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_m}\right)$$

We call both the Legendre and the Jacobi symbols *quadratic residue symbols*, and may freely use the same notation for each, as their definitions coincide whenever the odd positive integer b in the Jacobi symbol is prime.

We now follow the argument of [IR13, Chapter 5, §2] to assert the correctness of Algorithm 3.1. First, we refer the reader to a necessary lemma outlining the properties of the quadratic residue symbol. A proof is given in the reference.

Proposition 3.2 ([IR13, Proposition 5.2.2])**.** *Let b be an odd, positive integer.*

(a) $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$

(b) $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$

(c) *If a is odd and positive, then*

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$$

Proposition 3.3. *Algorithm 3.1 is correct.*

Proof. Need to proofreed this. It's long and I'm not sure how coherent it is. We adapt the proof of [IR13, Theorem 5.2.3]. First, consider the case where $n \geq 1$; that is, $M \neq 2$ is divisible by an odd prime. Since the sets $\{\ell_1, \ldots, \ell_k\}$ and $\{q_1, \ldots, q_n\}$ are disjoint sets of odd primes, the integers $2, \ell_1, \ldots, \ell_k, q_1, \ldots, q_n$ are pairwise coprime. Therefore, by the Chinese Remainder Theorem (Theorem 2.1), the integer b exists. Since $b \equiv 1 \pmod 8$, we know that b is odd, and write $b = p_1 \cdots p_m$, where the p_j are (not necessarily distinct) odd primes. To proceed, it is necessary to show that (i) $\left(\frac{2}{b}\right) = 1$, and (ii) $\left(\frac{q_i}{b}\right) = \left(\frac{b}{q_i}\right)$ for each $i = 1, \ldots, n-1$.

(i) By Proposition 3.2 (c),

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = (-1)^{\frac{(b+1)(b-1)}{8}}$$

As $8 \mid b-1$, the numerator is a multiple of $b+1$, which is even. Hence $\left(\frac{2}{b}\right) = 1$ as desired.

(ii) Consider some arbitrary q_i. We have that

$$\left(\frac{q_i}{b}\right) = \left(\frac{b}{q_i}\right) \iff \left(\frac{q_i}{b}\right)\cdot\left(\frac{b}{q_i}\right) = 1 \qquad ((\tfrac{\cdot}{\cdot}) \text{ is a map into } \{\pm 1\}) \tag{7}$$

$$\iff (-1)^{((q_i-1)/2)((b-1)/2)} = 1 \qquad \text{(Proposisiton 3.2 (c))} \tag{8}$$

$$\iff \frac{q_i-1}{2}\cdot\frac{b-1}{2} \text{ is even} \tag{9}$$

As $8 \mid b-1$, we have $4 \mid \frac{b-1}{2}$, so equation (9). Hence, $\left(\frac{q_i}{b}\right) = \left(\frac{b}{q_i}\right)$ as desired.

From this, we see:

$$\left(\frac{M}{b}\right) = \left(\frac{2}{b}\right)^e \left(\frac{q_1}{b}\right)\cdots\left(\frac{q_{n-1}}{b}\right)\left(\frac{q_n}{b}\right) \qquad \text{(as } (\tfrac{\cdot}{b}) \text{ is a homomorphism)} \tag{10}$$

$$= \left(\frac{q_1}{b}\right)\cdots\left(\frac{q_{n-1}}{b}\right)\left(\frac{q_n}{b}\right) \qquad \text{(by (i))} \tag{11}$$

$$= \left(\frac{b}{q_1}\right)\cdots\left(\frac{b}{q_{n-1}}\right)\left(\frac{b}{q_n}\right) \qquad \text{(by (ii))} \tag{12}$$

We again recall that $\left(\frac{\cdot}{q_i}\right)$ is a homomorphism with domain $\mathbb{Z}/q_i\mathbb{Z}$. Therefore, for each $i = 1, \ldots, n-1$, we have $\left(\frac{b}{q_i}\right) = \left(\frac{q_i}{b}\right) = 1$, where this last equality follows as $b \equiv 1 \equiv 1^2 \pmod{q_i}$. We also obtain that $\left(\frac{b}{q_n}\right) = \left(\frac{s}{q_n}\right) = -1$ since s is a non-residue modulo q_n by assumption. Continuing from equation (12), we conclude that $\left(\frac{M}{b}\right) = -1$. Applying the definition of the Jacobi symbol, we finally arrive at the equation

$$-1 = \left(\frac{M}{b}\right) = \left(\frac{M}{p_1}\right)\cdots\left(\frac{M}{p_m}\right) \tag{13}$$

Therefore, we necessarily have $\left(\frac{M}{p_j}\right) = -1$ for at least one j $(1 \le j \le m)$. Moreover, by inspection of the congruences giving the construction of b, no p_j for which M is a quadratic non-residue is contained in $\{\ell_1, \ldots, \ell_k\}$. By Euler's Criterion (Theorem 3.4), the desired primes p_j are exactly those for which $M^{(p-1)/2} \equiv -1 \pmod{p_j}$. Hence, the algorithm is correct in this case.

It remains to show that the algorithm is correct when $M = 2$. To proceed, we show that (iii) no $\ell \in \{\ell_1, \ldots, l_k\}$ divides b, and (iv) $\left(\frac{M}{b}\right) = -1$.

(iii) Recall that r is the product of all the elements $\{\ell_1, \ldots, \ell_k\}$ (which are odd primes) that are greater than 3. If $\ell = 3$, we see immediately that $3 \nmid r$, and hence $3 \nmid 8r+3 = b$. Otherwise, $\ell > 3$, implying that $\ell \mid r$, so

$$\ell \mid b \implies \ell \mid 8r+3 \implies \ell \mid 3,$$

which is absurd. Hence, in either case, $\ell \nmid b$ as desired.

(iv) Since $M = 2$, Proposition 3.2 gives

$$\left(\frac{2}{b}\right) = -1 \iff (-1)^{(b^2-1)/8} = -1 \iff \frac{b^2-1}{8} \text{ is odd} \iff 16 \nmid b^2 - 1$$

Of course,

$$b^2 - 1 \equiv (8r+3)^2 \equiv 8^2r^2 + 2\cdot 8r\cdot 3 + 3^3 \equiv 9 \pmod{16}$$

as desired.

Write $b = p_1 \cdots p_m$, where the p_j are (not necessarily distinct) odd primes. As before, we necessarily have $\left(\frac{M}{p_j}\right) = -1$ for at least one j. Moreover, (ii) shows that none of the primes dividing p are contained in $\{\ell_1, \ldots, \ell_k\}$, so the result follows. □

Corollary 3.1. *There are infinitely many inert primes in the ring of integers of any quadratic number field* $\mathbb{Q}(\sqrt{M})$.

Proof. Suppose not; that is, the finitely many inert primes are $\{\ell_1, \ldots, \ell_k\}$. Let S be the output of Algorithm 3.1 on the input M, $\{\ell_1, \ldots, \ell_k\}$, and any quadratic non-residue s modulo the largest prime dividing M (which is guaranteed to exist by Lemma 3.3). But we know that S contains at least one inert prime, a contradiction. □

4 Modular Algorithms in the Quadratic Integers

Having given an algorithm to compute the (infinitely many) inert primes of an arbitrary ring of quadratic integers, we now show that Garner's Chinese remainder theorem algorithm generalises to the quadratic integers. An immediate result of having Chinese remaindering over the quadratic integers is that the modular linear solver presented in §2.2 is also valid over the quadratic integers.

Recall from §2.1 that Garner's algorithm constructs the coefficients $v_0, v_1, \ldots, v_n$ of the mixed-radix representation equation (3). We present a recursive algorithm (Algorithm 4.1) to compute these coefficients in a more general setting, assuming that we have an algorithm to compute the required inverses.

Algorithm 4.1 Garner's Mixed Radix Coefficients

Input: For an integral domain R with characteristic 0, $u_0, u_1, \ldots, u_n \in R$, and $m_0, m_1, \ldots, m_n \in \mathbb{Z} \subseteq R$ generating comaximal ideals of R.

Output: $v_0, v_1, \ldots, v_n \in R$ with $u_i - (v_0 + v_1(m_0) + \cdots + v_n(\prod_{i=0}^{n-1} m_i)) \in \langle m_i \rangle$, $i = 1, \ldots, n$.

1:
2: **if** $n = 0$ **then**
3: $\quad v_0 \leftarrow u_0$
4: **else**
5: $\quad v_0, v_1, \ldots, v_{n-1} \leftarrow$ recursive call on $u_0, u_1, \ldots, u_{n-1}$ and $m_0, m_1, \ldots, m_{n-1}$
6: $\quad v_n \leftarrow \left(u_n - \sum_{i=0}^{n-1} v_i \prod_{j=0}^{i-1} m_i\right) \left(\prod_{j=0}^{n-1} m_j\right)^{-1} \mod \langle m_n \rangle$
7: **end if**
8: **return** $v_0, v_1, \ldots, v_n$

Proposition 4.1. *Algorithm 4.1 is correct.*

Proof. Since Algorithm 4.1 is recursive and does not mutate any of its variables, we may prove correctness using induction. Formally, we prove that for all $n \in \mathbb{N}$, the output $v_0, v_1, \ldots, v_n$ of the algorithm satisfies

$$P(n) \quad \iff \quad u_k \equiv v_0 + v_1(m_0) + v_2(m_0 m_1) + \cdots + v_n \prod_{j=0}^{n-1} m_j \mod \langle m_k \rangle \quad \forall k = 0, 1, \ldots, n. \tag{14}$$

The base case is $n = 0$. Here, we have $P(0) \iff u_0 \equiv v_0 \mod \langle m_i \rangle$. On input $n = 0$, algorithm computes $v_0 = u_0$, and $P(0)$ follows immediately. Now let $n > 0$ be arbitrary and suppose $P(n-1)$. Therefore, the mixed-radix coefficients $v_0, v_1, \ldots, v_{n-1}$ produced by the recursive call on line 5 satisfy

$$u_k \equiv v_0 + v_1(m_0) + v_2(m_0 m_1) + \cdots + v_{n-1} \prod_{j=0}^{n-2} m_j \mod \langle m_k \rangle \quad \forall k = 0, 1, \ldots, n-1. \tag{15}$$

Take v_n as computed by line 6. Given equation (15), to show that the congruences of equation (14) are satisfied for each $k = 0, 1, \ldots, n-1$, it is sufficient to show that

$$v_n \prod_{j=0}^{n-1} m_j \equiv 0 \mod \langle m_k \rangle . \tag{16}$$

Since $k < n$, we see that m_k divides the product in equation (16), giving the result immediately. Finally, for $k = n$ (noting that all inverses are taken modulo $\langle m_n \rangle$):

$$\begin{aligned}
& v_0 + v_1(m_0) + v_2(m_0 m_1) + \cdots + v_n \prod_{j=0}^{n-1} m_j \\
& \quad \equiv \sum_{i=1}^{n-1} v_i \prod_{j=0}^{i-1} m_j + \left(u_n - \sum_{i=1}^{n-1} v_i \prod_{j=0}^{i-1} m_j \right) \left(\prod_{j=0}^{i-1} m_j \right)^{-1} \left(\prod_{j=0}^{i-1} m_j \right) && \mod \langle m_n \rangle \\
& \quad \equiv \sum_{i=1}^{n-1} v_i \prod_{j=0}^{i-1} m_j + \left(u_n - \sum_{i=1}^{n-1} v_i \prod_{j=0}^{i-1} m_j \right) && \mod \langle m_n \rangle \\
& \quad \equiv u_n && \mod \langle m_n \rangle ,
\end{aligned}$$

Therefore $P(n)$, so Algorithm 4.1 is correct by induction. □

Corollary 4.1. *Algorithm 4.1 correctly computes the Garner mixed-radix coefficients when R is a ring of quadratic integers.*

Proof. Since $\mathbb{Z} \subset \mathbb{Z}[\gamma] = R$, we know that R has characteristic 0. [Mar77, Theorem 14] gives us that R is an integral domain and that the (non-zero) prime ideals are maximal. Since inert primes are integers that generate prime ideals in R, we conclude distinct inert primes indeed generate comaximal ideals of R.

Finally, we need to give an algorithm to compute inverses modulo inert primes $\langle m \rangle$. Of course, Proposition 3.1 tells us that there is an isomorphism $\phi : R \to (\mathbb{Z}/p\mathbb{Z})[x]/\langle f \rangle$ (a map for which we can easily compute images and inverse) for some irreducible polynomial f. We summarise our algorithm in a diagram:

$$\begin{array}{ccc} R/\langle m\rangle^* & \xrightarrow{(\cdot)^{-1}} & R/\langle m\rangle^* \\ {\scriptstyle\phi}\downarrow & & \uparrow{\scriptstyle\phi^{-1}} \\ (\mathbb{Z}/p\mathbb{Z})[x]/\langle f\rangle^* & \xrightarrow[\rho]{} & (\mathbb{Z}/p\mathbb{Z})[x]/\langle f\rangle^* \end{array}$$

The map ρ computes inverses, and is given by $\rho(h+\langle f\rangle) = s+\langle f\rangle$, where $hs+ft = 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ (noting that $s,t \in (\mathbb{Z}/p\mathbb{Z})[x]$ exist and are computed by the extended Euclidean algorithm). □

On inspection, we see that the modular linear solver that we presented over $\mathbb{Q}$ (Algorithm 2.1) only depends on having some way to produce arbitrarily many distinct primes, the ability to do arithmetic modulo those primes, and a Chinese remainder algorithm. We have shown that we have exactly these tools in $\mathbb{Q}(\sqrt{M})$, as long as we restrict ourselves to the inert primes. Up to adjusting the bound on the product of the primes in Algorithm 2.1, there is no need to give an additional proof that the algorithm is correct for $\mathbb{Q}(\sqrt{M})$. We use this (somewhat incredible) result to conclude this section with an example of using a modular algorithm to solve a linear system over $\mathbb{Q}(\sqrt{122})$, using small machine (inert) primes.

Example 4.1. Let

$$A = \begin{pmatrix} 81-19\sqrt{122} & 78-89\sqrt{122} & -81-80\sqrt{122} \\ 22-53\sqrt{122} & -8+66\sqrt{122} & -43-19\sqrt{122} \\ 50-30\sqrt{122} & -90+154\sqrt{122} & -2-124\sqrt{122} \end{pmatrix}, \qquad b = \begin{pmatrix} 26851-2700\sqrt{122} \\ -41098+883\sqrt{122} \\ -67029+1076\sqrt{122}. \end{pmatrix}$$

Running Algorithm 2.1 solves the system $Ax = b$ using seven 16-bit inert primes, and reconstructs $D = \det A$ and a scaled-up solution vector y into 57-bit integers (which fit into machine words)! The solution vector x is then given by

$$x = y/D = \begin{pmatrix} \frac{5\sqrt{122}}{2} \\ \frac{33}{2} - 3\sqrt{122} \\ 15 \end{pmatrix}$$

Notably, the modular solver uses only machine integers, and all operations can be performed within machine integers. Solving the same system using fraction-free Gaussian elimination requires 105-bit integers. ■

5 Conclusion

In this report, we introduced the concept of modular algorithms over $\mathbb{Z}$ (and $\mathbb{Q}$), including an example of a modular linear solver. We gave a method to generalise these algorithms to rings of quadratic integers using inert primes; giving an algorithm to construct inert primes, a Chinese remaindering algorithm for working modulo inert primes, and a result characterising arithmetic modulo these inert primes. Finally, we showed that we can use the same modular linear solver presented for $\mathbb{Q}$ to solve systems in $\mathbb{Q}(\sqrt{M})$.

The linear solver presented is much slower (over $\mathbb{Q}$) than other known methods, such as one using p-adic lifting and rational reconstruction [Dix82]. There may be potential for these methods to be generalised to the quadratic integers; particularly rational reconstruction, which could be used to lift results from $(\mathbb{Z}/p^k\mathbb{Z})[\gamma]$ into $\mathbb{Q}[\gamma] = \mathbb{Q}(\sqrt{M})$ (where γ is as in Theorem 3.1).

6 References

[CL77] S Cabay and TPL Lam. Congruence techniques for the exact solution of integer systems of linear equations. *ACM Transactions on Mathematical Software (TOMS)*, 3(4):386–397, 1977.

[Cra50] Gabriel Cramer. *Introduction à l'analyse des lignes courbes*. Cramer, 1750.

[Dix82] John D Dixon. Exact solution of linear equations using p-adic expansions. *Numerische Mathematik*, 40(1):137–141, 1982.

[Gar59] Harvey L Garner. The residue number system. In *Papers presented at the the March 3-5, 1959, western joint computer conference*, pages 146–153, 1959.

[GCL92] Keith O Geddes, Stephen R Czapor, and George Labahn. *Algorithms for computer algebra*. Springer Science & Business Media, 1992.

[IR13] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer Science & Business Media, 2013.

[Mar77] D.A. Marcus. *Number Fields*. Springer-Verlag, 1977.

[TI61] H Takahasi and Y Ishibashi. A new method for 'exact computation' by a digital computer. In *Inf. Processing in Japan*, pages 28–42, 1961.