# Finding a perfect square in and in

## 1 Definition of Smoothness on and

**Definition 1**: A rational factor base is a finite collection of prime numbers.

In this paper, only rational factor bases of small, consecutive primes are considered. Therefore, for the purposes of this this paper, a rational factor base can be thought of as a set:

**Definition 2**: An integer is said to be smooth over a rational factor base if contains of the prime divisors of .

Note that in the numerical example, all of the numbers {455, 39270,770, 429, 1616615, 3990, 106590, 187, 19019} were smooth over the rational factor base {2, 3, 5, 7, 11, 13, 17, 19}.

It is now necessary to define an algebraic factor base, a concept very similar to a rational factor base. However, some things must be assumed in order to properly define an algebraic factor base.

**Definition 3**: An algebraic factor base is a finite set where for , each satisfies such that . This condition causes to be what is commonly called a “*prime ideal*”.

Definition 4: an element is said to be smooth over an algebraic factor base if such that .

The definition of an algebraic factor involves elements . is a difficult space to represent on a computer, and hence development of an algorithm based on would be difficult. Fortunately, this concept of an algebraic factor base has an analog that gives a way to more easily represent elements .

**Theorem 1**: Let be a polynomial with integer coefficients and let be a root of . Then the set of pairs where is a prime integer and , where is in bijective correspondence with the set of that satisfy the criteria for being in an algebraic factor base.

This theorem can be used to represent the algebraic factor base as a finite set of pairs of integers . While not every element of can be represented as a pair , what can be represented is sufficient to meet the needs of the GNFS.

## 2 Finding Smooth Numbers - Sieving Techniques

In order to find a square in and in , it first necessary to find pairs of number such that is smooth in some algebraic factor base and is smooth in some rational factor base.

Let be an arbitrary rational factor base represented by the set of primes and Let be an arbitrary algebraic factor base in represented by the set of pairs .

**Theorem 2**: For in an algebraic factor base and that has the representation , divides if and only if .

**Theorem 3**: A finite set of pairs represents a complete factorization of if and only if where is the degree of .

**Theorem 4**: A prime number will divide if and only if .

Using the above three theorems, smooth elements of and can be found in the following way:

1. Fix , and let be an arbitrary positive integer.
2. Let vary from to . Create two arrays: one for the various values of that will result and another for various values of that will result. This concept is illustrated in Figure 1.

Figure 1. Sieve Arrays

1. For each in , will divide if and only if . Find values of for which for some , and for each value of make note of this factor of in the sieve array. Repeat this process for each . When finished, make note of all the in the sieve array that are completely factored by this method. These are smooth in .
2. Proceed in an identical manner for the sieve array. An divides if and only if . Find values of satisfying for some . For each found, make note of this factor of in the sieve array. When finished, for all in the sieve array there will be a list of factors. If then this list of factors is a complete factorization and hence is smooth over the given algebraic factor base .
3. Compare the two arrays entry by entry. At any position, if both the and are smooth then this is what was sought after. Save it for later use.

One can repeat this procedure by altering b to find as many satisfying the required criteria as may be needed.

## 3 Verifying That Elements of and are Squares

From the above section, we can find smooth and smooth . In this section, we will introduce one method to find squares in and . First of all, it is necessary to develop methods for testing for squareness in and .

It is relatively easy to determine whether or not an arbitrary is a perfect square. In fact, the methods used in the GNFS will give access to the prime factorization of for the that is to be tested for squareness. In this case, is a perfect square if and only if every exponent occurring in the prime factorization is even. That is, for every exponent in the prime factorization, if then is a perfect square in . Testing for perfect squareness is more complicated.

**Theorem 5**: Let have the factorization where for every , satisfies the criteria to be in an algebraic factor base. If is a perfect square in then , .

This is one such condition that a perfect square will satisfy. However, it is not the only condition.

**Definition 4**: The Legendre symbol for and a prime integer is defined as:

**Theorem 6**: Let be a set of pairs such that is a perfect square in . Then for any with prime and as Theorem 1 with for any ,

Note that in the above theorem, implies that . Thus and so . This is an important observation to make as it will be used in later sections.

The above two theorems give necessary but not sufficient conditions for an element of to be a perfect square. That is, if the goal is to show that something is a perfect square, then the above theorems are the converse of what is needed.

In practice, one determines if an element is square in the following way:

1. Verify that for a factorization for every .
2. Let be a set of pairs of numbers with prime and given as in Theorem 1. Choose such that for every occurring in the factorization of . Verify that for every , , for defined as in Theorem 6. The set is called the quadratic character base and each is called a quadratic character.
3. If the above two conditions are satisfied, then is probably a perfect square in . Note that to increase this probability, one should increase the number of elements in .

In summary, there are now developed methods for testing for perfect squares in and .

## 4 Putting it All Together: From Smooth Numbers to Square Numbers

Up to this point methods are developed to find a set of numbers such that is smooth in rational factor base and is smooth in rational factor base . This section will describe how to use this information to find a square in and .

Let the rational factor base have elements, and let the algebraic factor base have elements. Choose an arbitrary quadratic character base with elements. and will be used to find a square in and , and will be used to verify that the result is a square.

Each can be represented as a row vector with entries. The first entry should be equal to 0 if is positive and 1 if is negative. The next entries are given to the exponent vector modulo 2, as described in last section. The following entries are used for indicating whether a particular element of divides .

The exponent on this element of that appears in the factorization module 2 is what should appear in each of these entries. The final entries are used in conjunction with the quadratic character base . Each entry is set to 0 if for the appropriate , . Otherwise, set the entry to 1.

In summary, let the rational factor base be , let the algebraic factor base be , and let the quadratic character base be . For a given , has a factorization . has the factorization that can be represented as .

Then the pair should be represented by a row vector of the following form:

Now suppose a is found such that is a perfect square in and is a perfect square in . Then the following must all hold:

1. must be positive. Let . Note that this is just the first entry in the vector for . Then is positive if and only if . This insures that the number of negative numbers in the product is even. Because -1 raised to an even power is 1, the product will be positive.
2. Every exponent occurring in the prime factorization of must be even. Because , is smooth on , the product will also be smooth on . Furthermore, if is the corresponding exponent appearing on any in the prime factorization of , then the exponent appearing in the prime factorization of the product is . Thus, for to be square, ,

Each in the sum on the left is an entry in the vector representation of .

1. Every exponent occurring in the prime ideal factorization of must be even. Similar to the above, , is smooth in implies that smooth in . Let have the representation . Then has the representation

Each exponent in this expansion is required to be even. Thus , . This implies that , . Note that each is just an entry in the vector representation .

1. For every , must be 1. Because , , in order for , the number of for which must be even. For a given , the vector representation of has an entry corresponding to

If the sum of these entries is even then the number of ’s for which will be even.

Hence

Because all 4 of the above condition must hold simultaneously, is a perfect square in and is a perfect square in if and only if the sum of the vector representation of each is equivalent to the zero vector modulo 2.

Let the set of smooth have elements. Let be a matrix with each row being equivalent to the vector representation of an .

Find a in order to get perfect squares is equivalent to finding a column vector such that

If , this congruence is guaranteed to have a nontrivial solution .

Because of this congruence modulo 2, every is in the set (the residue set of 2). Let the subset be defined by , if . Then is a perfect square in and is a perfect square in .

## 5 A summary of the above method