

Quadratic Factoring Sieve

Jonathan Lee*

June 26, 2002

Many numerical methods (not necessarily just those for integers) involve a sieve, whereby undesirable numbers are systematically ruled out in order to leave a particular set of numbers satisfying a particular property.

Perhaps the most simple of these is the Sieve of Eratosthenes, where multiples of primes (except for the prime itself) are crossed off, leaving at the end of the algorithm a table of uncrossed numbers corresponding to the primes in the respective interval.

This sieve can be enhanced to yield the factorizations of all numbers in a given interval with a simple modification – instead of crossing out the multiples of a prime, we simply repeatedly divide by the prime as many times as possible.

For determining the factorizations of the numbers in $[1, n]$, this is actually fairly efficient, with approximately $n \cdot \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p_{\pi(n)}}\right)$, or $n \cdot \sum_{i=1}^{\pi(n)} \frac{1}{p_i} \approx n \cdot \sum_{i=1}^{\pi(n)} \frac{1}{i \log i} \approx n \cdot \int_1^{\pi(n)} \frac{1}{x \log x} dx \approx n \cdot \log \log n = O(n \log \log n)$ steps. This is fairly efficient if do desire all factorizations for $m \in [1, n]$, but for n itself, we need a better method.

As its name implies, the method of factoring integers via the quadratic sieve involves quadratic terms, or those involving squares. We already know one such method, that is, the “difference of squares” identity, which states $a^2 - b^2 = (a + b) \cdot (a - b)$. Clearly, if we’re lucky enough to find $a, b \in \mathbb{Z}, a^2 - b^2 = n$, then factoring n is then trivialized.

Does such a factorization always exist? Suppose $n = ab, 2 \nmid a, b$. (Note that a and b need not be prime.) Then, $n = \left[\frac{1}{2}(a + b)\right]^2 - \left[\frac{1}{2}(a - b)\right]^2$, and such a difference of squares exists.

Since $n = a^2 - b^2 \iff a^2 - n = b^2$, we need only systematically try values for a until $a^2 - n$ is a square. (Using $n + b^2 = a^2$ instead would work equally well in theory; however, we will see that we wish to minimize our dependent variable.)

This is quite easy to check in \mathbb{Z} . Unfortunately, this method, due to Fermat, tends only to work well when b is small; ie., when n has two factors close to \sqrt{n} . (Note that there may be other “pairs of factors” as well.)

We can refine this method by relaxing the initial condition to $a^2 \equiv b^2 \pmod{n} \iff a^2 - b^2 = kn \quad k \in \mathbb{Z}$. Of course, this does not work well; for instance, if $a = b = 0$, we have nothing to work with. We thus impose the necessary and sufficient additional condition that $a \not\equiv \pm b \pmod{n}$.

Since $a^2 - b^2 \equiv 0 \pmod{n} \iff n \mid a^2 - b^2 = (a + b) \cdot (a - b)$, and that $a \not\equiv b \pmod{n} \iff n \nmid (a + b), (a - b)$, we obtain $d = \gcd(n, a - b) \neq 1$ to be a non-trivial factor of n and we are done. (Note that $a \equiv \pm b \pmod{n} \implies (a + b) \text{ or } (a - b) \equiv 0 \pmod{n} \implies n \mid (a + b)(a - b)$ trivially.)

It is important to note that, while trying different values of a , we have no way of determining *a priori* whether $a \equiv \pm b \pmod{n}$ for the resultant value of $b = \sqrt{a^2 - n} \in \mathbb{Z}$, if it even exists. This applies to the next refinement.

We now introduce the concept of factor bases. In determining whether a number is square, it is fairly useful to have a prime factorization, especially if we are to consider arbitrary products from a set of given numbers. For this purpose, we choose a $B < n$ and construct the prime factor base $F(B) = \{2, 3, 5, \dots, p_{\pi(B)}\} \cup \{-1\}$ consisting of the primes less than B in addition to -1 , which indicates sign.

With this factor base, we are able to define the concept of B -smooth numbers; that is, the integers factoring completely over $F(B)$. We may then represent each B -smooth integer $n = (-1)^{\lambda_0} \cdot \prod_{i=1}^{\pi(B)} p_i^{\lambda_i}$ by

*leej@math.usask.ca

a vector $\{\lambda_0, \lambda_1, \dots, \lambda_{\pi(n)}\} \in \mathbb{Z}^{\pi(n)+1}$, where $\mathbb{Z} = \mathbb{P} \cup \{0\}$. By inspection, n is a square in \mathbb{Z} iff each of its corresponding λ_i are even. As exponent parity is all we care about, we therefore reduce n to an exponent vector in $\mathbb{F}_2^{\pi(n)+1}$. (This defines a homomorphism $(\mathbb{Z}, *) \rightarrow (\mathbb{F}_2^{\pi(B)+1}, +)$).

We now briefly modify notation. For some a_i , define $c_i = a_i^2 - n$. (Compare this to $b_i = \sqrt{a_i^2 - n}$, though we do not make use of it.) Above, we sought an a such that b^2 (existed and) was a square. Now, we seek some $\{a_i\}$ such that $\prod_i c_i$ forms a square. By linear algebra and considering the reductions of the c_i to $\mathbb{F}_2^{\pi(B)+1}$, we're assured a linearly dependent set $\{c_i\}$ and thus a square $\prod_i c_i$ after no more than $\pi(B) + 2$ candidates for c_i .