The quadratic sieve

A simple way to look for x^2 with a smooth remainder modulo n is to take $x_0 = \lceil \sqrt{n} \rceil$ and try successive values $x = x_0, x_0 + 1, x_0 + 2, \ldots$ If $x = x_0 + t$ with t not too large then the remainder is $x^2 - n$, which will be of order $t\sqrt{n}$. This is more like $\sqrt{n}$ in size than n, and so will be more likely to be smooth than a random integer in $(0, n]$. If q is a prime divisor of $x^2 - n$ then n must be a quadratic residue of q, so that only half the primes need to be included in the factor base.

Rather than test $x^2 - n$ for smoothness by trial division the quadratic sieve uses a different technique to "sieve out" non-smooth values. In order to do this the factor base is extended to include powers of primes q^e up to b, and not just primes themselves. Then, to search values $L < x \leq U$ looking for cases in which $x^2 - n$ is b-smooth, we proceed as follows. We produce an array indexed by the integers x in our interval. Then, for each prime power q^e in our factor base we compute the solutions (usually two) of $x^2 = n (\mathrm{mod}\ q^e)$, and call them a and b. We then go through the array in steps of length q^e adding (an approximation to) $\log q$ for every $x = a (\mathrm{mod}\ q^e)$. We repeat this for integers $x = b (\mathrm{mod}\ q^e)$, and then move on to the next prime power. This is the **sieving** process.

Once we are done, we check though the contents of the array, looking for places where the value is (approximately) $\log(x^2 - n)$, in which case $x^2 - n$ must be composed of prime factors $q \leq b$. We can then decompose these smooth values into their prime factorization by trial division, but this step need only be done for the few numbers we actually want, rather than for every single value $x^2 - n$.

A crude estimate for the time requirement of the sieve process uses the fact that there are at most $2(1 + (U - L)/q^e)$ values of x to be visited for each prime power q^e. Thus the time taken is

$$O\left(\sum_{q^e \leq b} (1 + (U - L)/q^e)\right) = O(b) + O((U - L)\log b).$$

For comparison, trial division for takes time $O(b)$ for each value of x, yielding a far worse total $O((U - L)b)$.

The number field sieve

The number field sieve was introduced by Pollard in 1988. It is the fastest algorithm currently available. However its complexity means that it is a substantial task to implement it. A number n has to be very large before the number field sieve is faster than other methods. We will describe it in its simplest form.

Choose two monic irreducible polynomials $f_1, f_2 \in \mathbb{Z}[x]$ with smallish coefficients, and a common root, m say, modulo n. We want the degrees to be small, but not too small. One easy way to achieve this is to begin by picking a degree d, asymptotically of size $(\log n)^{1/3}(\log\log n)^{-1/3}$ (but this might be 5 or 6 in practice), and to take m about $n^{1/d}$ or just under. Now write n in base m as

$$n = m^d + a_{d-1}m^{d-1} + \ldots + a_0,$$

so that $0 \leq a_i < m$. We then take $f_1(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0$ and $f_2(x) = x - m$. A random polynomial is almost certainly irreducible, but if we are unlucky with f_1 we can try another m.

Consider the number field $\mathbb{Q}(\theta)$ where θ is a root of f_1. Then $\mathbb{Z}[\theta]$ is a subring of the ring of integers for $\mathbb{Q}(\theta)$. Unfortunately:-

(i) $\mathbb{Z}[\theta]$ may not be the full ring of integers;

(ii) Even if it is, it may not be a unique factorization domain; and

(iii) The unit group is infinite, if $d \geq 3$.

We will ignore these problems in this brief description!

We now have two ring homomorphisms:

$$\phi_1 : \mathbb{Z}[\theta] \to \mathbb{Z}/n\mathbb{Z} \quad \text{given by} \quad \phi_1 : \theta \mapsto \overline{m} = m + n\mathbb{Z},$$

and

$$\phi_2 : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \quad \text{given by} \quad \phi_2 : k \mapsto \overline{k} = k + n\mathbb{Z}.$$

We aim to find a set I of pairs (a, b) of coprime integers, such that $\prod_{(a,b)\in I}(a - \theta b)$ is a square α^2 in the ring $\mathbb{Z}[\theta]$, and also $\prod_{(a,b)\in I}(a - bm)$ is a square k^2 in $\mathbb{Z}$. If we can do this then

$$\phi_1(\beta)^2 = \prod_{(a,b)\in I} \phi_1(a - b\theta) = \prod_{(a,b)\in I} (\overline{a} - \overline{b}\overline{m}) = \prod_{(a,b)\in I} \phi_2(a - bm) = \phi_2(k)^2.$$

This produces two integer squares whose difference is divisible by n, and we can hope that this will enable us to split n.

To find a suitable set I we choose factor bases for $\mathbb{Z}[\theta]$ and $\mathbb{Z}$. For the former, the factor base will consist of a basis for the units, together with a set of prime ideals with norm below some smoothness bound. We then try lots of pairs (a, b), looking for cases where both $a - b\theta$ and $a - bm$ are smooth in their respective senses, and hence can be decomposed into "primes" from the respective factor bases. One can sieve, as with the quadratic sieve, to speed this process.
Having gathered enough relations, in which both $a - b\theta$ and $a - bm$ are smooth, we use linear algebra over $\mathbb{F}_2$ to find a subset of the pairs such that the products $\prod_{(a,b)\in I}(a - \theta b)$ and $\prod_{(a,b)\in I}(a - mb)$ are both squares.

The whole process is rather like the smooth square factoring algorithm of Section 3.10, or the quadratic sieve, except that it is done over a number field. The technical problems are considerable, but in the calculation of the expected running time everything depends on the size of m, rather than n (if d is chosen around $(\log n)^{1/3}(\log\log n)^{-1/3}$). The outcome is that one has an expected running time of

$$O(\exp(c(\log n)^{1/3}(\log\log n)^{2/3}))$$

which is asymptotically better than any other current method.

We conclude with a simple example, courtesy of Richard Pinch.
$n = 84101 = 290^2 + 1$.

Take $d = 2$, $m = 290$, $f_1(x) = x^2 + 1$, $f_2(x) = x - 290$.

Then our number field is $\mathbb{Q}(i)$, and the ring we work in is $\mathbb{Z}[i]$ which fortunately is the full ring of integers, is a Unique Factorization Domain, and has only the units ± 1 and $\pm i$.

Taking $a = -38$, $b = -1$ we have $a - ib = -38 + i = -(2 + i)(4 - i)^2$, and $a - mb = 2^2.3^2.7$
Taking $a = -22$, $b = -19$, we have $a - ib = -22 + 19i = -(2 + i)(3 - 2i)^2$ and $a - mb = 2^4.7^3$

It follows that

$$(-38 + i)(-22 + 19i) = \big((2 + i)(4 - i)(3 - 2i)\big)^2 = (31 - 12i)^2$$

and

$$(-38+m)(-22+19m) = 2^6.3^2.7^4 = 1176^2.$$

Then $\phi_1(31-12i) = \overline{31-22m} = -\overline{3449}$ and $\phi_2(1176) = \overline{1176}$, whence $3449^2 = 1176^2 (\text{mod } 84101)$.

We therefore calculate $\gcd(3449-1176, 84101)$, giving us a value 2273, and we find that $84101 = 2273 \times 37$.