Factorization of Integers

Notes for talks given at London South Bank University

20 February, 19 March, 2008

Tony Forbes

ADF37A version 1.7A

THE PROBLEM

Given a positive integer N, find a positive integer d, $1 < d < N$ such that $d|N$.

TRIAL DIVISION

Think of a number, d; see if $d|N$. For example, take $N = 15$. Try $2, 3, \ldots, 14$ in turn. Behold, $3|15$ and a factor is discovered.

If N is big, this is the only viable method. The world record is the 746190-digit prime factor $3 \cdot 2^{2478785} + 1$ of the Fermat number $2^{2^{2478782}} + 1$ (Cosgrave, Jobling, Woltman & Gallot, 2003).

FERMAT'S METHOD

If $N = a^2 - b^2$, then N has the factorization $(a - b)(a + b)$ and moreover if N is odd, it works the other way: $N = uv \Rightarrow N = \left(\frac{1}{2}(u + v)\right)^2 - \left(\frac{1}{2}|u - v|\right)^2$.

So we look for factors by trying values of b in $N + b^2$ and seeing if a perfect square results.

For example, $15 + 1^2 = 16 = 4^2$; so $a = 4$, $b = 1$, $15 = 3 \cdot 5$.

SHOR'S ALGORITHM

Another way of factorizing 15 appears to have been demonstrated by Scientists at IBM's Almaden Research Center in 2001. They built a small quantum computer and used the following algorithm due to Peter Shor.

Assume N is composite. Choose $a < N$, $\gcd(a, N) = 1$. Find r, the period of the function

$$f : x \mapsto a^x \bmod N;$$

that is, find the smallest $r > 0$ for which $a^r \equiv 1 \pmod{N}$.

Assume r is even and $a^{r/2} \not\equiv \pm 1 \pmod{N}$; otherwise start again with a new a. Then, since $(a^{r/2} - 1)(a^{r/2} + 1) = a^r - 1 \equiv 0 \pmod{N}$, $\gcd(a^{r/2} - 1, N)$ is a non-trivial factor of N.

For example, $N = 15$, $a = 2$ gives $r = 4$, $\gcd(2^2 - 1, 15) = 3$ and $\gcd(2^2 + 1, 15) = 5$.

The determination of r is particularly suited to quantum computing. For details, see [2, section 8.5.2], or look up 'Shor's algorithm' in *Wikipedia*.

Before moving on to greater things, and to avoid silly cases that might otherwise present themselves, let us agree from now on that the number N to be factorized has the following properties: (i) N is not divisible by anything that could cause trouble—in particular, we shall always assume that N is odd and not divisible by 3; (ii) N is not a square or higher power of an integer; (iii) N is composite; (iv) N is not too small.

Testing (i) is trivial—in practice one would trial-divide N by everything up to some convenient limit. Condition (ii) can be done quickly by Newton's method for extracting roots. For (iii), most of the time one can apply Fermat's Little Theorem: find a such that $a^N \not\equiv a \pmod{N}$.

THE QUADRATIC SIEVE

For a sequence of numbers x_1, x_2, ..., we compute

$$a_i \;=\; x_i^2 \bmod N, \qquad i = 1, 2, \ldots,$$

and we look for a set of these congruences where the product of the a_i is a square, say $\prod_j a_{i_j} = y^2$. Then we have $x^2 = \prod_j x_{i_j}^2 \equiv \prod_j a_{i_j} = y^2 \pmod N$ and this will hopefully lead to a non-trivial factor of N via $x \pm y$.

Example. $N = 38413$: start at $x_1 = \lceil \sqrt{N} \rceil = 196$.

i	x_i	$x_i^2 \bmod N$	factorization of $x_i^2 \bmod N$	2	3	7	11
1	196	$196^2 \equiv 3 \pmod N$	3	0	1	0	0
2	197	$197^2 \equiv 396 \pmod N$	$2^2 \cdot 3^2 \cdot 11$	0	0	0	1
3	198	$198^2 \equiv 791 \pmod N$	$7 \cdot 113$				
4	199	$199^2 \equiv 1188 \pmod N$	$2^2 \cdot 3^3 \cdot 11$	0	1	0	1

From entries 1, 2 and 4 we have $196^2 \cdot 197^2 \cdot 199^2 \equiv 3 \cdot 396 \cdot 1188 \equiv 1188^2$ giving $x = 196 \cdot 197 \cdot 199 = 7683788$, $y = 1188$, $x - y = 7682600$, $x + y = 7684976$. But $\gcd(7682600, N) = 38413 = N$ and $\gcd(7684976, N) = 1$. So nothing achieved here. We continue.

i	x_i	$x_i^2 \bmod N$	factorization of $x_i^2 \bmod N$	2	3	7	11
5	200	$200^2 \equiv 1587 \pmod N$	$3 \cdot 23^2$				
6	201	$201^2 \equiv 1988 \pmod N$	$2^2 \cdot 7 \cdot 71$				
7	202	$202^2 \equiv 2391 \pmod N$	$3 \cdot 797$				
8	203	$203^2 \equiv 2796 \pmod N$	$2^2 \cdot 3 \cdot 233$				
9	204	$204^2 \equiv 3203 \pmod N$	3203				
10	205	$205^2 \equiv 3612 \pmod N$	$2^2 \cdot 3 \cdot 7 \cdot 43$				
11	206	$206^2 \equiv 4023 \pmod N$	$3^3 \cdot 149$				
12	207	$207^2 \equiv 4436 \pmod N$	$2^2 \cdot 1109$				
13	208	$208^2 \equiv 4851 \pmod N$	$3^2 \cdot 7^2 \cdot 11$	0	0	0	1

The appearance of entry 13 is helpful. We can take entries 2 and 13 to get $197^2 \cdot 208^2 \equiv 396 \cdot 4851 \equiv 1386^2$. Now $x = 197 \cdot 208 = 40976$, $y = 1386$, $x - y = 39590$, $x + y = 42362$. Then $\gcd(39590, N) = 107$ and $\gcd(42362, N) = 359$ yields the two prime factors of N.

A Practical Algorithm

Choose a suitable bound B. Make a list, $\mathcal{Q}$, of 2 and all odd primes q for which $q \le B$ and $(N/q) = 1$. The set $\mathcal{Q}$ is called the *factor base*. Let $\mathcal{Q} = \{q_1, q_2, q_3, \ldots, q_k\}$, with $q_1 = 2$.

Create a set $\mathcal{U}$ of numbers of the form $x^2 \bmod N$, $x \in [\sqrt{N}, \sqrt{2N}]$, which have no prime factors $> B$, so-called B-*smooth* numbers. By restricting x we simplify the calculation of $x^2 \bmod N$. Indeed, $x^2 \bmod N = x^2 - N$ for $x \in [\sqrt{N}, \sqrt{2N}]$. We include the condition $(N/q) = 1$ since for q odd, $q | x^2 - N \Rightarrow (N/q) = 1$.

Now we think of the numbers in $\mathcal{U}$ as the elements of a vector space $\mathcal{V}$ of dimension $k = |\mathcal{Q}|$ over $\mathbb{F}_2$ thus:

$$q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k} \in \mathcal{U} \leftrightarrow (\alpha_1, \alpha_2, \ldots, \alpha_k) \bmod 2 \in \mathcal{V}.$$

If $\mathcal{V}$ has more than k elements, we use standard linear algebra to look for linear combinations of vectors of $\mathcal{V}$ that sum to the zero vector. For any such linear combination

of elements of $\mathcal{V}$, the product of the corresponding elements of $\mathcal{S} \subseteq \mathcal{U}$ will be a perfect square, Y^2, say. Thus we will have $X^2 \equiv Y^2 \pmod{N}$, where X is the product of the xs for which $x^2 \bmod N \in \mathcal{S}$, and we hope that one of $X \pm Y$ will contain a prime factor of N. This won't always happen, so when building $\mathcal{U}$, it is wise to collect few more than $k+1$ items.

The name *quadratic sieve* refers to the ingenious manner in which $\mathcal{U}$ is built.

We make a long list, $\mathcal{L} = (L_1, L_2, \dots)$, of numbers $L_i = \log(x_i^2 - N)$, for a range of consecutive x_i in $[\sqrt{N}, \sqrt{2N}]$. On the first time through, the list will correspond to the values $x_i = \lfloor \sqrt{N} \rfloor + i$, $i = 1, 2, \dots$.

For each prime $q \in \mathcal{Q}$ we compute the roots $x = \pm a$ of $x^2 - N \equiv 0 \pmod{q}$. But note that when $q = 2$ the roots are both equal to 1. Let's first deal with a.

Find the smallest j such that $x_j \equiv a \pmod{q}$. Subtract $\log q$ from L_j and every L_{j+mq}, $m = 1, 2, \dots$ in the list $\mathcal{L}$. This process is called *sieving*—we are sieving the list $\mathcal{L}$ by a modulo q.

We need to sieve $\mathcal{L}$ by a modulo q^α for powers $\alpha = 1, 2, \dots$, each time subtracting $\log q$. And if $q^\alpha > 2$, we repeat the sieving for the other root, $-a$.

Using the unarithmetical function log is just a way of avoiding division during the sieving. There is no loss of performance since the relevant logarithms can be pre-computed. Great accuracy is not needed with the logarithms of the sieving primes. In fact one can get away with integer-only arithmetic by using just the length of the number in bits.

When all the sieving has been done for each prime $q \in \mathcal{Q}$, we look at what remains in $\mathcal{L}$. Those L_i which have been reduced to zero are precisely the ones that correspond to the B-smooth values of $x_i^2 - N$ that we want to collect in $\mathcal{U}$.

Optional extras

The large prime option

The choice of B is rather delicate. If B is too small, finding the B-smooth numbers for $\mathcal{U}$ is going to be difficult. But a large B requires a large matrix for performing the linear algebra on.

We can gain a little extra by collecting, in addition to B-smooth numbers, those $x_i^2 - N$ which are products of primes up to B plus at most one extra prime in the range (B, B^2). These extra numbers are available for free, with no need to do any more sieving. We look for L_i which have final values in the range $(0, 2 \log B)$. The corresponding $x_i^2 - N$ must have the form $q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k} Q$ with $Q \in (B, B^2)$.

So for each prime $Q \in (B, B^2)$, we collect all those $x_i^2 - N$ which are of the form $q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k} Q$. If there are none, there is nothing to do. If there is just one, we discard it. If there are more than one, namely $x_i^2 - N = y_i$, $i = 1, 2, \dots, m$, we combine them in pairs, $x_1 x_i \equiv y_1 y_i \pmod{N}$, and we can legitimately add $y_1 y_i$ to $\mathcal{U}$ and the vector for $y_1 y_i / Q^2$ to $\mathcal{V}$, $i = 2, 3, \dots, m$.

Two large primes

The large prime option can usefully be extended to two large primes at a cost of some complexity. Here we allow $x^2 - N$ to take values of the form $q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k} Q_1 Q_2$, where $q_i \le B$, $i = 1, 2, \dots, k$ and $B < Q_1, Q_2 < B^2$.

Centred sieving interval

We sieve over an interval centred on $\lceil \sqrt{N} \rceil$. This produces more smaller values of $x^2 - N$ but they come with both positive and negative signs. To cope with the negative values we add -1 to the factor base. This works precisely because the product of 0 modulo 2 negatives is positive.

Ignore prime powers

Sieving over squares and higher powers of not-too-small primes is not usually necessary because numbers divisible by them are not very common. The saving in sieving costs outweighs the loss of a few B-smooth $x^2 - N$ numbers that might have been found if the sieving were done properly.

The next innovation is important enough to justify an entirely separate section.

THE MULTIPLE POLYNOMIAL QUADRATIC SIEVE

In the quadratic sieve, we let x range over values from $\lceil\sqrt{N}\rceil$ on. Although $x^2 - N$ starts small it increases rapidly. Since finding large B-smooth numbers is a lot harder than finding small ones, it is desirable to keep the numbers being tested as small as possible.

The multiple polynomial quadratic sieve, we use several functions $ax^2 + 2bx + c$ instead of just $x^2 - N$.

Let us assume that x ranges over the interval $[-\ell, \ell]$. We choose a, b, c such that $a > 0$ is a square times a B-smooth number, $a \approx \sqrt{2N}/\ell$, $b^2 \equiv N \pmod{a}$, $0 < b < a/2$, and $c = (b^2 - N)/a$.

One way of choosing a suitable a is to take a prime $p \approx (2N)^{1/4}/\sqrt{\ell}$ with $(p/N) = 1$ and put $a = p^2$; then $b^2 \equiv N \pmod{a}$ has precisely two solutions, $\pm$something, and we can take for b the one which is in $(0, a/2)$.

Let $f(x) = ax^2 + 2bx + c$. Then

$$af(x) = a^2x^2 + 2abx + ac = (ax + b)^2 - N.$$

Hence $(ax+b)^2 \equiv af(x) \pmod{N}$, and since we already know that a is a square, we seek values of $f(x)$ which are B-smooth with the intention of using linear methods to combine them together to create squares, exactly as in the plain quadratic sieve.

Also, $f(\pm\ell) \approx (a^2\ell^2 - N)/a \approx N/a$ and $f(0) = c \approx -N/a$. Thus on the interval $[-\ell, \ell]$, $f(x)$ is bounded by $\ell/\sqrt{2} \cdot \sqrt{N}$. Compare with the polynomial $x^2 - N$ as in the ordinary quadratic sieve; if $x \in [-\ell, \ell]$, the corresponding bound is $2\ell \cdot \sqrt{N}$.

The improvement gained by multiple polynomials is significant. For instance, It is known that when N has about 100 digits, MPQS runs about 17 times faster than QS.

THE POLLARD ρ METHOD

Define a quadratic function $f(x) = x^2 + a$, where a is a smallish fixed positive constant. Choose an initial starting-point, b, and generate two sequences S_i, T_i, defined by

$$S_0 = T_0 = b, \quad S_i = f(S_{i-1}) \mod N, \quad T_i = f(f(T_{i-1})) \mod N, \quad i = 1, 2, \ldots.$$

Basically the sequences are same except that T_i is going twice as fast as S_i: $T_i = S_{2i}$ for $i = 0, 1, \ldots$. We look for a factor of N by computing $\gcd(T_i - S_i, N)$.

Given a prime factor d of N, what value of k do we need such that the collection of k consecutive values of S_i has probability $1/2$ of containing a duplicate modulo d? If one thinks of S_i as a random sequence, one can argue as in the 'birthday paradox' to obtain the value $k \approx \sqrt{d}$ for large d. So we can reasonably expect to find a factor of size d after about $\sqrt{d}$ iterations of S_i and T_i.

The precise nature of the function $f(x)$ is not important. It only has to create a sequence that looks random enough for the theory to apply. Linear functions don't work.

THE FAST FOURIER TRANSFORM

Working in a suitable ring, let X be a D-dimensional vector $(X_0, X_1, \ldots, X_{D-1})$ and let ω be a primitive Dth root of 1 in the ring. We define the *finite Fourier transform*, $\hat{X} = (\hat{X}_0, \hat{X}_1, \ldots, \hat{X}_{D-1})$ by

$$\hat{X}_k = \sum_{j=0}^{D-1} \omega^{kj} X_j, \qquad k = 0, 1, \ldots, D-1.$$

If we are working in $\mathbb{C}$, we use $\omega = \exp(2\pi i/D)$. But there is an interesting alternative. We can work in the ring $\mathbb{Z}_F$, where $F = 2^{2^n} + 1$, the nth Fermat number. Let D be a not-too-large power of two, say $D = 2^\delta$ and let $\omega = 2^{2^{n-\delta+1}}$. Then we have

$$\omega^D = 2^{2^{n-\delta+1}2^\delta} = 2^{2^{n+1}} = (2^{2^n})^2 \equiv (-1)^2 \equiv 1 \pmod{F}.$$

It is advantageous to have D as large as possible. If $D = 2^{n+1}$, we can set $\omega = 2$, but we can actually go up one more power of two. If $D = 2^{n+2}$, then $\omega = \sqrt{2}$ and indeed the square root does exist: $\sqrt{2} = 2^{3\cdot 2^{n-2}} - 2^{2^{n-2}}$. We cannot extend D to 2^{n+3} for $n = 5, 6$ and 7 because $\sqrt[4]{2}$ does not exist modulo F_5, F_6 and F_7, although it does for F_8.

When D is a power of two, the *fast Fourier transform* is a method of computing the finite Fourier transform. We consider triply indexed numbers $X_{d,j,k}$ which satisfy

$$\begin{aligned} X_{d,k,j} &= X_{2d,k,j} + \omega^{dk} X_{2d,k,j+d}, \\ X_{d,k+\frac{D}{2d},j} &= X_{2d,k,j} - \omega^{dk} X_{2d,k,j+d}, \end{aligned}$$

where $d = \frac{D}{2}, \frac{D}{4}, \ldots, 2, 1$, $j = 0, 1, \ldots, d-1$ and $k = 0, 1, \ldots, \frac{D}{2d} - 1$.

Theorem 1 (the fast Fourier transform) *Let*

$$\begin{aligned} X &= (X_0, X_1, \ldots, X_{D-1}), \\ \hat{X} &= (\hat{X}_0, \hat{X}_1, \ldots, \hat{X}_{D-1}), \end{aligned}$$

where D is a power of two. Suppose $X_j = X_{D,0,j}$, $j = 0, 1, \ldots, D-1$. Then $\hat{X}_k = X_{1,k,0}$, $k = 0, 1, \ldots, D-1$.

Proof. Work an example with $D = 8$, say. The theorem will become obvious. □

Fast multiplication

We use the FFT to compute the product xy. Let

$$x = X_0 + X_1 M + \cdots + X_{D-1} M^{D-1}, \qquad 0 \le X_0, X_1, \ldots, X_{D-1} < M,$$

and

$$y = Y_0 + Y_1 M + \cdots + Y_{D-1} M^{D-1}, \qquad 0 \le Y_0, Y_1, \ldots, Y_{D-1} < M,$$

for some suitable number base M, and define the product vector $A \otimes B$ by

$$[A \otimes B]_j = A_j B_j, \quad j = 0, 1, \ldots, D-1.$$

Then if the ring is $\mathbb{C}$, or if the ring is $\mathbb{Z}_F$ and $(DM)^2 < F$, we have

$$xy \equiv \frac{1}{D} \sum_{h=0}^{D-1} \widehat{[\hat{X} \otimes \hat{Y}]}_{-h \bmod D} M^h \pmod{M^D - 1}.$$

THE NUMBER FIELD SIEVE

This section is based on [2, section 6.2]. Let

$$f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$$

be an irreducible polynomial with integer coefficients, and let α be one of the roots of $f(x)$. Let ϕ be the homomorphism from $\mathbb{Z}[\alpha]$ to the number ring $\mathbb{Z}_N$, defined by $\phi(\alpha) = m$ for some integer m such that $f(m) \equiv 0 \pmod N$. Curiously, although the number α plays a very important role in what follows, for computations we can survive without ever knowing what it actually is.

Given the degree d (the value $\lfloor (3 \log N / \log\log N)^{1/3} \rfloor$ is suggested by complexity analysis), we construct the polynomial $f(x)$ by setting $m = [N^{1/d}]$ and writing N in base m,

$$N = m^d + c_{d-1}m^{d-1} + \cdots + c_1m + c_0, \qquad 0 \le c_0, c_1, \ldots, c_{d-1} < m.$$

Then we define $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$, using the same coefficients. We must check $f(x)$ for irreducibility; but if $f(x)$ turns out to be reducible, $f(x) = f_1(x)f_2(x)$, say, then we have a non-trivial factorization of $N = f(m) = f_1(m)f_2(m)$. So we can assume that $f(x)$ is irreducible.

Now suppose we have a set $\mathcal{S}$ of coprime integer pairs (a, b) such that

$$\prod_{(a,b)\in\mathcal{S}} (a - b\alpha) = \gamma^2 \quad \text{and} \quad \prod_{(a,b)\in\mathcal{S}} (a - bm) \equiv w^2 \pmod N \tag{1}$$

for some $\gamma \in \mathbb{Z}[\alpha]$ and some integer w. Let $\phi(\gamma) \equiv u \pmod N$. Then

$$u^2 \equiv \phi(\gamma)^2 \equiv \phi(\gamma^2) \equiv \prod_{(a,b)\in\mathcal{S}} \phi((a - b\alpha)) \equiv \prod_{(a,b)\in\mathcal{S}} (a - bm) \equiv w^2 \pmod N.$$

Thus we have $u^2 \equiv w^2 \pmod N$ from which a factor might be found via $u \pm w$.

For the first condition in (1), it is too difficult to work with $(a - b\alpha)$ directly, so instead we consider its *norm*. Suppose $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ are the roots of $f(x)$ in $\mathbb{C}$. Define

$$\mathrm{Norm}(x_0 + x_1\alpha + \cdots + x_{d-1}\alpha^{d-1}) = \prod_{j=1}^{d} (x_0 + x_1\alpha_j + \cdots + x_{d-1}\alpha_j^{d-1}).$$

Write

$$F(x, y) = x^d + c_{d-1}x^{d-1}y + \cdots + c_1xy^{d-1} + c_0y^d, \qquad G(x, y) = x - ym.$$

Then

$$\mathrm{Norm}(a - b\alpha) = (a - b\alpha_1)\ldots(a - b\alpha_d) = b^d\left(\frac{a}{b} - \alpha_1\right)\ldots\left(\frac{a}{b} - \alpha_d\right) = b^d f\left(\frac{a}{b}\right) = F(a, b).$$

Proceeding as in MPQS, we want to find a set $\mathcal{U}$ of coprime pairs (a, b) such that $F(a, b)G(a, b)$ is B-smooth and that (1) holds for some $\mathcal{S} \subseteq \mathcal{U}$.

For the $G(x, y)$ part, we associate with $G(a, b) = (-1)^{e_0}p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$ a vector of zeros and ones, $\mathbf{v}^G(a, b) = (e_0, e_1, e_2, \ldots, e_k) \bmod 2$, just as for MPQS, except that since $G(x, y)$ is linear we use all the $\pi(B)$ primes up to B.

The part involving $F(x, y)$ is not so easy to deal with. The main problem is that $\mathrm{Norm}(\beta)$ square does not necessarily imply that β is a square in $\mathbb{Z}[\alpha]$.

For each prime p, we need to consider the set $R(p)$ of integers $r \in [0, p-1]$ where $f(r) \equiv 0 \pmod{p}$. Then for $\gcd(a,b) = 1$ and prime p,

$$p|F(a,b) \qquad \text{iff} \qquad a \equiv br \pmod{p} \text{ for some } r \in R(p).$$

Indeed $p|F(a,b) \Leftrightarrow b^d \equiv 0$ or $f(a/b) \equiv 0 \Leftrightarrow a^d \equiv 0$ or $a/b \equiv r \pmod{p}$.

In the vector space, it is not sufficient to record the parity of the exponent of p in $F(a,b)$; we need the root r as well. Thus we record the exponent of p under the pair (p,r).

Let's look at a simple example. Let $f(x) = x^2 + 1$. Then $\alpha = i$, $R(2) = \{1\}$, $R(3) = \{\ \}$, $R(5) = \{2,3\}$, and the exponent vectors corresponding to $F(x,y)$ for 5-smooth numbers will have coordinates for $(b,r) = (2,1),(5,2),(5,3)$. Some typical values of $F(a,b)$ are shown in the following table.

	a	b	$F(a,b) = \text{Norm}(a-bi)$	exponent vector (p,r) (2,1)	(5,2)	(5,3)
1	3	1	$F(3,1) = 10$	1	0	1
2	3	−1	$F(3,-1) = 10$	1	1	0
3	2	1	$F(2,1) = 5$	0	1	0
4	2	−1	$F(2,-1) = 5$	0	0	1
5	1	1	$F(1,1) = 2$	1	0	0
6	1	−1	$F(1,-1) = 2$	1	0	0

Looking at entries 1, 4 and 5, the sum of the exponent vectors is zero modulo 2, and the product $(3-i)(2+i)(1-i) = (3-i)^2$ corresponding to $F(3,1)F(2,-1)F(1,1) = 100$ is a square in $\mathbb{Z}[i]$. On the other hand, the product of entries 1, 3 and 5, $(3-i)(2-i)(1-i) = -10i$ is not a square, even though its norm $F(3,1)F(2,1)F(1,1) = 100$ is.

We now formalize these ideas. Let us say that $a-b\alpha$ is B-smooth if $\text{Norm}(a-b\alpha) = F(a,b)$ is B-smooth. For coprime a,b we associate with B-smooth $a-b\alpha$ a vector $\mathbf{v}^F(a,b)$ that has entries $\mathbf{v}^F_{p,r}(a,b)$ for each pair p,r where $p \le B$, $R(p)$ is non-empty and $r \in R(p)$. If $a \not\equiv br \pmod{p}$, we set $\mathbf{v}^F_{p,r}(a,b) = 0$; otherwise $a \equiv br \pmod{p}$ and $\mathbf{v}^F_{p,r}(a,b)$ is the exponent modulo 2 of p in the prime factorization of $F(a,b)$.

Unfortunately this does not always work. The problem is that the ring we should really be using is not $\mathbb{Z}[\alpha]$ but the possibly bigger ring $\mathcal{I}$ of algebraic integers in the field $\mathbb{Q}(\alpha)$.

It is well known (see, for example, [3]) that the non-zero ideals of $\mathcal{I}$ have unique factorization. We extend the definition of norm to ideals. If J is a non-zero ideal of $\mathcal{I}$ we define $\text{Norm}(J) = |\mathcal{I}/J|$, the number of elements in the finite quotient ring $\mathcal{I}/J$. The definition is completed by defining the norm of the zero ideal as zero. If J_1 and J_2 are ideals in $\mathcal{I}$ then $\text{Norm}(J_1J_2) = \text{Norm}(J_1)\text{Norm}(J_2)$. Moreover this norm is compatible with the norm of an element of $\mathcal{I}$; if $\beta \in \mathcal{I}$, then $\text{Norm}((\beta)) = |\text{Norm}(\beta)|$.

Let us see what the components $\mathbf{v}^F_{p,r}(a,b)$ represent. First we look at the ideal $(p, \alpha - r)$.

For p prime and $r \in R(p)$, let $P_1, P_2, \ldots, P_k$ be the prime ideals of $\mathcal{I}$ that divide $(p, \alpha - r)$. Observe that $\text{Norm}(\alpha - r) = \pm f(r) \equiv 0 \pmod{p}$ — so $(p, \alpha - r)$ is not the unit ideal. Hence there are positive integers $e_1, e_2, \ldots, e_k$ such that $\text{Norm}(P_j) = p^{e_j}$ for $j = 1, 2, \ldots, k$. However, if p does not divide the index of $\mathbb{Z}[\alpha]$ in $\mathcal{I}$ (in particular, if $\mathbb{Z}[\alpha] = \mathcal{I}$) then $k = 1$, $e_1 = 1$ and $(p, \alpha - r) = P_1$.

Suppose $r' \in R(p)$ and $r' \neq r$. Since $r - r'$ is coprime to p, the prime ideals that divide $(p, \alpha - r)$ are different from the prime ideals that divide $(p, \alpha - r')$; i.e. $(p, \alpha - r)$ is coprime to $(p, \alpha - r')$. Moreover, if a and b are integers, then $a - b\alpha \in (p, \alpha - r)$ if and only if $a \equiv br \pmod{p}$; indeed, $a - b\alpha \in (p, \alpha - r) \Leftrightarrow a - br = a - b\alpha + b(\alpha - r) \in (p, \alpha - r) \Leftrightarrow p|a - br$.

Suppose a and b are coprime and $a \equiv br \pmod{p}$. If P is a prime ideal of $\mathcal{I}$ that divides both (p) and $(a - b\alpha)$, then P divides $(p, \alpha - r)$, and hence $P = P_j$ for some j. To see this, write $c = b^{-1} \mod p$. Then, since $a \equiv br \pmod{p}$, $a - b\alpha = a - br - b(\alpha - r) \in P$. Hence $b(\alpha - r) \in P$, therefore $bc(\alpha - r) \in P$ from which it follows that $\alpha - r \in P$. Thus P divides $(p, \alpha - r)$.

To summarize what we have done so far, we have

$$\begin{gathered}
r \not\equiv r' \pmod{p} \Rightarrow (p, \alpha - r) \text{ and } (p, \alpha - r') \text{ are coprime;} \\
P_1, P_2, \ldots, P_k \mid (p, \alpha - r), \qquad \mathrm{Norm}(P_j) = p^{e_j}, \quad j = 1, 2, \ldots, k; \\
(p, \alpha - r) | (a - b\alpha) \Leftrightarrow (a - b\alpha) \subseteq (p, \alpha - r) \Leftrightarrow a \equiv br \pmod{p}; \\
a \equiv br \pmod{p}, P|(p) \text{ and } P|(a - b\alpha) \Rightarrow P = P_j \text{ for some } j,\ 1 \le j \le k.
\end{gathered}$$

Given p prime, $r \in R(p)$, and that $P_1, P_2, \ldots P_k$ are the prime ideal divisors of $(p, \alpha - r)$, suppose a and b are coprime and that $P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k}$ appears in the prime factorization of $(a - b\alpha)$ with $a_j \ge 0$, $j = 1, 2, \ldots, k$. Suppose $a_i > 0$. Then $P_i | (p, \alpha - r)$ and hence $a \equiv br \pmod{p}$. But then $(p, \alpha - r) | (a - b\alpha)$. Hence $P_1 P_2 \ldots P_k | (a - b\alpha)$. Thus if any of the a_i are positive, then $a \equiv br \pmod{p}$ and all the a_i positive, and no other prime ideal divides both (p) and $(a - b\alpha)$. So the (p, r) part of the norm of $a - b\alpha$ is precisely the norm of $P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k}$. Thus

$$p^{\mathbf{v}^F_{p,r}(a,b)} = \mathrm{Norm}(P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k}) = p^{e_1 a_1 + e_2 a_2 + \cdots + e_k a_k}. \tag{2}$$

Let $\mathbf{v}^F_P(a, b)$ denote the exponent of the prime ideal P in the prime ideal factorization of $(a - b\alpha)$. Then (2) gives

$$\mathbf{v}^F_{p,r}(a, b) = \sum_{j=1}^{k} e_j \, \mathbf{v}^F_{P_j}(a, b). \tag{3}$$

We are now ready to prove the following lemma.

Lemma 1 *If $\mathcal{S}$ is a set of coprime integer pairs (a, b) such that each $a - b\alpha$ is B-smooth, and if $\prod_{(a,b)\in\mathcal{S}}(a - b\alpha)$ is the square of an element of $\mathcal{I}$, the ring of algebraic integers of $\mathbb{Q}(\alpha)$, then*

$$\sum_{(a,b)\in\mathcal{S}} \mathbf{v}^F(a, b) \equiv 0 \pmod{2}. \tag{4}$$

Proof [2, Lemma 6.2.1]. If $\prod_{(a,b)\in\mathcal{S}}(a - b\alpha)$ is a square in $\mathcal{I}$, then the principal ideal it generates is the square of an ideal. So for every prime ideal P in $\mathcal{I}$, we have that $\sum_{(a,b)\in\mathcal{S}} \mathbf{v}^F_P(a, b)$ is even. Hence

$$\sum_{(a,b)\in\mathcal{S}} \mathbf{v}^F_{p,r}(a, b) = \sum_{j=1}^{k} e_j \sum_{(a,b)\in\mathcal{S}} \mathbf{v}^F_{P_j}(a, b).$$

Since the P_j are prime ideals, the inner sum on the right is even. Hence the left-hand side is even. □

Let us continue with the example given in the table on page 7. Recall that $f(x) = x^2 + 1$, $\alpha = i$, $R(2) = \{1\}$, $R(3) = \{\}$, $R(5) = \{2, 3\}$. Also for computations with ideals it is helpful to have these prime factorizations in $\mathbb{Z}[i]$:

$$\begin{gathered}
2 = (1 + i)(i - 1) = -i(1 - i)^2, \qquad 5 = (2 + i)(2 - i), \\
3 - i = -(2 + i)(1 - i), \qquad 3 + i = (2 - i)(1 + i).
\end{gathered}$$

Now we can extend the table as follows.

	a	b	$F(a,b)$	p	r	$(p, \alpha - r)$	$(a - b\alpha)$
1	3	1	10	5	3	$(5, i-3) = (2+i)$	
				2	1	$(2, i-1) = (1-i)$	$(3-i) = ((2+i)(1-i))$
2	3	-1	10	5	2	$(5, i-2) = (2-i)$	
				2	1	$(2, i+1) = (1-i)$	$(3+i) = ((2-i)(1-i))$
3	2	1	5	5	2	$(5, i-2) = (2-i)$	$(2-i)$
4	2	-1	5	5	3	$(5, i-3) = (2+i)$	$(2+i)$
5	1	1	2	2	1	$(2, i-1) = (1-i)$	$(1-i)$
6	1	-1	2	2	1	$(2, i-1) = (1-i)$	$(1+i) = (1-i)$

For instance, consider $F(3,1)$; $a = 3, b = 1$. There are two (p, r) pairs to deal with.
(i) $p = 5$, $r = 3$. We have

$$(p, \alpha - r) = (5, i-3) = ((2+i)(2-i), (2+i)(-1+i)) = (2+i);$$

so $k = 1$, $P_1 = (2+i)$, $e_1 = 1$ and $\mathrm{Norm}(P_1) = 5$.
(ii) $p = 2$, $r = 1$. Now

$$(p, \alpha - r) = (2, i-1) = ((1-i)^2, (1-i)) = (1-i);$$

so again $k = 1$ and $e_1 = 1$ but this time $P_1 = (1-i)$ and $\mathrm{Norm}(P_1) = 2$.
Moreover, we have the factorization $(a - b\alpha) = (3-i)$ into prime ideals $(2+i)$ times $(1-i)$. The rest of the table is constructed in a similar manner.

Lemma 1 is fine; unfortunately for our purposes it is upside down. But let's forget about that for the moment. Suppose that (4) holds and let $\sigma = \prod_{(a,b)\in\mathcal{S}}(a - b\alpha)$. There are a few problems that need addressing before we make any useful deductions about σ being a square.
(i) If the ring $\mathbb{Z}[\alpha]$ is the same as $\mathcal{I}$, then the ideal (σ) in $\mathcal{I}$ is the square of some ideal J in $\mathcal{I}$. But if the ring $\mathbb{Z}[\alpha]$ is not the same as $\mathcal{I}$, then it may not be the case that (σ) is the square of an ideal in $\mathcal{I}$.
(ii) Even if $(\sigma) = J^2$ for some ideal J in $\mathcal{I}$, J need not be a principal ideal.
(iii) Even if $(\sigma) = (\gamma)^2$ for some $\gamma \in \mathcal{I}$, it may not be that $\sigma = \gamma^2$.
(iv) Even if $\sigma = \gamma^2$ for some $\gamma \in \mathcal{I}$, it may not be that γ is in $\mathbb{Z}[\alpha]$.

Lemma 2 *Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with root $\alpha \in \mathbb{C}$. Let $\mathcal{I}$ be the ring of algebraic integers in $\mathbb{Q}(\alpha)$ and let $\beta \in \mathcal{I}$. Then $f'(\alpha)\beta \in \mathbb{Z}[\alpha]$.*

Proof. See [2, Lemma 6.2.3]. □
This takes care of problem (iv). Suppose $\sigma = \prod_{(a,b)\in\mathcal{S}}(a - b\alpha)$ is a square in $\mathcal{I}$, say γ^2. Then by Lemma 2, $f'(\alpha)\gamma \in \mathbb{Z}[\alpha]$ and hence $f'(\alpha)^2\sigma$ is a square in $\mathbb{Z}[\alpha]$.
Consider problem (i). Suppose $\sigma = \prod_{(a,b)\in\mathcal{S}}(a - b\alpha)$ is a square in $\mathcal{I}$ but that the prime ideal factorization of σ does not have all even exponents. Then it is 'well known' that those prime ideals with odd exponents must divide the index of $\mathbb{Z}[\alpha]$ in $\mathcal{I}$. So their number is small, and is bounded by $\log_2[\mathcal{I} : \mathbb{Z}[\alpha]]$.
Problem (ii) possibly occurs when the class group of $\mathcal{I}$ is non-trivial. Call two ideals I, J of $\mathcal{I}$ *equivalent* if there exist principal ideals P, Q of $\mathcal{I}$ such that $PI = QJ$. The *class group* is set of equivalence classes $[I]$ of ideals of $\mathcal{I}$ together with the operation defined by $[I][J] = [IJ]$. Its order is called the *class number*. But the group of ideals relevant to

problem (ii) is the ideal class group modulo the subgroup of squares of ideal equivalence classes. The rank of this group is bounded by the base-2 logarithm of the class number.

Problem (iii) occurs when the group of units over the subgroup of squares of units is non-trivial. The rank of this group is bounded by d, the degree of $f(x)$.

Hence we see that in some sense problems (i), (ii) and (iii) are small, and we could just quietly forget about them, perhaps remembering to collect more sieved numbers for analysis in the hope that eventually one of them will work. However, there is a device (due to Adleman) which works much better.

Lemma 3 *Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with root $\alpha \in \mathbb{C}$. Suppose q is an odd prime and that s is an integer such that $f(s) \equiv 0 \pmod{q}$ and $f'(s) \not\equiv 0 \pmod{q}$. Let $\mathcal{S}$ be a set of coprime integer pairs (a, b) such that q does not divide any $a - bs$ for $(a, b) \in \mathcal{S}$ and that $f'(\alpha)^2 \prod_{(a,b)\in\mathcal{S}}(a - b\alpha)$ is a square in $\mathbb{Z}[\alpha]$. Then*

$$\prod_{(a,b)\in\mathcal{S}} \left(\frac{a - bs}{q}\right) = 1. \tag{5}$$

Proof. Consider the homomorphism $\phi_q : \mathbb{Z}[\alpha] \to \mathbb{Z}_q$, $\phi_q : \alpha \mapsto s$ [2, Lemma 6.2.4]. □

Thus we have two necessary conditions for $f'(\alpha)^2 \prod_{(a,b)\in\mathcal{S}}(a - b\alpha)$ being a square in $\mathbb{Z}[\alpha]$, namely (4) and (5). Adleman's idea is to pretend that they are sufficient.

We augment the exponent vector $\mathbf{v}^F$ with some new pairs (q_j, s_j), where q_j is an odd prime such that $f(s_j) \equiv 0 \pmod{q_j}$ and q_j does not divide any of the $\text{Norm}(a - b\alpha)$ for $(a, b) \in \mathcal{S}$. So $q_j > B$. Then we set

$$\mathbf{v}^F_{q_j,s_j}(a, b) = \begin{cases} 0 & \text{if } \left(\dfrac{a - bs_j}{q_j}\right) = 1 \\ 1 & \text{if } \left(\dfrac{a - bs_j}{q_j}\right) = -1. \end{cases}$$

If the number of new pairs (q_j, s_j) is not too small, then the augmented vectors $\mathbf{v}^F$ will be sufficient to ensure that squares constructed by the linear algebra stage really are squares most of the time. With a bit of arm-waving, it turns out that $\lfloor 3 \log_2 N \rfloor$ new pairs would be more than sufficient for practical purposes.

Suppose we have done the sieving and the linear algebra. So we have at this point a set $\mathcal{S}$ of coprime pairs (a, b) such that

$$\begin{aligned} f'(\alpha)^2 \prod_{(a,b)\in\mathcal{S}} (a - b\alpha) &= \gamma^2 \quad \text{for } \gamma \in \mathbb{Z}[\alpha], \\ \prod_{(a,b)\in\mathcal{S}} (a - bm) &= w^2 \quad \text{for } w \in \mathbb{Z}. \end{aligned}$$

If u is an integer with $\phi(\gamma) \equiv u \pmod{N}$, then $u^2 \equiv (f'(m)\, w)^2 \pmod{N}$, which with luck generates a factorization of N via $\gcd(u - f'(m)\, w, N)$.

Finding w is easy; it is computed modulo N from the known prime factorization of w^2. However, the problem remains of finding γ, the square root of γ^2. It can be done but the details are not so easy—see [2, section 6.2.5]—and I am happy to omit them.

AN ALGORITHM FOR THE NUMBER FIELD SIEVE

As a summary of everything we have done, we offer the following procedure for factorizing N. This is based on [2, Algorithm 6.2.5].

Setting up

Let $d = \lfloor (3 \log N / \log\log N)^{1/3} \rfloor$. Thus $d = 5$ for $N \approx 10^{100}$, $d = 6$ for $N \approx 10^{200}$ and $d = 7$ for $N \approx 10^{330}$. However, MPQS is faster for $N < 10^{100}$.

Let $B = \lfloor \exp\left((8/9)^{1/3} (\log N)^{1/3} (\log\log N)^{1/3}\right) \rfloor$, as suggested by complexity analysis.

Let $m = \lfloor N^{1/d} \rfloor$.

Define the coefficients c_j by $N = m^d + c_{d-1} m^{d-1} + \cdots + c_1 m + c_0$, $0 \le c_j < m$.

Let $f(x) = x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + c_0$.

Attempt to factorize $f(x)$ in $\mathbb{Z}[x]$. If there is a non-trivial factorization $f(x) = f_1(x) f_2(x)$, report a successful factorization $N = f_1(m) f_2(m)$ and stop.

Let $F(x, y) = x^d + c_{d-1} x^{d-1} y + \cdots + c_1 x y^{d-1} + c_0 y^d$.

Let $G(x, y) = x - my$.

For each prime $p \le B$, compute $R(p) = \{r \in [0, p-1] : f(r) \equiv 0 \pmod{p}\}$.

Let $T = \lfloor 3 \log_2 N \rfloor$.

Find T pairs $(q_1, s_1), (q_2, s_2), \ldots, (q_T, s_T)$ such that $q_1, q_2, \ldots, q_T > B$, $s_j \in R(q_j)$ and $f'(s_j) \not\equiv 0 \pmod{q_j}$.

Let $B' = \sum_{p \le B} |R(p)|$.

Let $U = 1 + \pi(B) + B' + T$.

The sieve

Use a sieve to find a set $\mathcal{U}$ of at least U coprime pairs (a, b) such that $a \neq 0$ and $F(a, b) G(a, b)$ is B-smooth.

The matrix

Here we construct a $|\mathcal{U}| \times U$ binary matrix, one row for each (a, b) pair. Each row consists of $\mathbf{v}(a, b)$, the exponent vector modulo 2 for (a, b). The vector has $U = 1 + \pi(B) + B' + T$ binary entries made up as follows.

(i) The first bit of $\mathbf{v}$, namely $\mathbf{v}_0^G(a, b)$, is 1 if $G(a, b) < 0$; otherwise 0.

(ii) The next $\pi(B)$ bits are set according to the $\pi(B)$ primes $p \le B$. If $p^{e_p} \mid G(a, b)$ but $p^{e_p+1} \nmid G(a, b)$, then the bit for p in $\mathbf{v}$, namely $\mathbf{v}_p^G(a, b)$ is set to $e_p \bmod 2$.

(iii) The next B' bits are set according to the pairs (p, r), where p is a prime not exceeding B and $r \in R(p)$. Let $\mathbf{v}_{p,r}^F(a, b)$ denote the bit for (p, r). If $a \equiv br \pmod{p}$, then $\mathbf{v}_{p,r}^F(a, b)$ is the exponent modulo 2 of p in the prime factorization of $F(a, b)$; otherwise $\mathbf{v}_{p,r}^F(a, b) = 0$.

(iv) The next T bits are set according to the pairs (q_j, s_j). Let $\mathbf{v}_{q_j,s_j}^F(a, b)$ denote the bit for (q_j, s_j). If $((a - bs_j)/q_j) = -1$, then $\mathbf{v}_{q_j,s_j}^F(a, b)$ is set to 1; otherwise $\mathbf{v}_{q_j,s_j}^F(a, b) = 0$.

Linear algebra

Using linear algebra over $\mathbb{F}_2$, find a non-empty set $\mathcal{S} \subseteq \mathcal{U}$ such that $\sum_{(a,b) \in \mathcal{S}} \mathbf{v}(a, b) = 0$.

Use the known prime factorization of the integer square $\prod_{(a,b) \in \mathcal{S}} (a - bm)$ to find a residue $w \bmod N$ such that $\prod_{(a,b) \in \mathcal{S}} (a - bm) \equiv w^2 \pmod{N}$.

By some method, try to find a square root $\gamma \in \mathbb{Z}[\alpha]$ of $f'(\alpha)^2 \prod_{(a,b) \in \mathcal{S}} (a - b\alpha)$. If successful, compute $y = \phi(\gamma)$ by the substitution $\alpha \to m$.

Compute $\gcd(y - f'(m)\, w, N)$ and hope that it is a non-trivial factor of N.

SOME NOTABLE FACTORIZATIONS

Trial division

$3 \cdot 2^{2478785} + 1$ (746190 digits) divides $2^{2^{2478782}} + 1$; Cosgrave, Jobling, Woltman, Gallot, 2003.

$7 \cdot 2^{2167800} + 1$ (652573 digits) divides $2^{2^{2167797}} + 1$; Cooper, Jobling, Woltman, Gallot 2007.

Pollard ρ method

6192864263277076981 (19 digits) divides $2^{2386} + 1$; Harvey Dubner.

1059099980653317121 (19 digits) divides $6^{1049} - 1$; Harvey Dubner.

Pollard $p - 1$ method

137209840691013934741147397829773702964959958384316465015 3 (58 digits) divides $2^{2098}+1$; Paul Zimmermann.

3575614199333163052319359756325100920067071981903146884 97 (57 digits) divides $6^{396}+1$; Paul Zimmermann.

Elliptic curve method

444434979215670990789575255179863190894618060876873794628023807 8881 (67 digits) divides $10^{381} + 1$; B. Dodson, ECMNET, 2006.

4659775785220018543264560743076778192897 (40 digits) divides $F_{10} = 2^{1024}+1$; R. Brent, 1995.

Quadratic sieve

(135-digit factor of $2^{1606}+1$) = (66-digit prime) $\times$ (69-digit prime); Dodson, A. K. Lenstra, Leyland, Muffett, Wagstaff.

(124-digit factor of $2^{895} - 1$) = (52-digit prime) $\times$ (73-digit prime); Jens Franke.

Number field sieve

$2^{1039} - 1 = 5080711 \times$ (80-digit prime) $\times$ (227-digit prime); 313 digits, K. Aoki, J Franke, T. Kleinjung, A. K. Lenstra, D. A. Osvik, 2007. Sieving took about 285 GHz years. After a filtering step the result was a 66718354×66718154 matrix. The linear algebra step took another 105 GHz years. The first three solutions produced trivial factors. The fourth solution produced the desired factorization. [http://eprint.iacr.org/2007/205.ps].

$6^{353} - 1 = 5 \times$ (120-digit prime) $\times$ (155-digit prime); 275 digits, Aoki, Kida, Shimoyama, Ueda, 2006.

$F_9 = 2^{512} + 1 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times$ (99-digit prime); 155 digits, A. K. Lenstra, H. W. Lenstra, M. S. Manasse, J. M. Pollard, 1990. The number actually factorized was $f(m) = 8F_9$, where $f(x) = x^5+8$ and $m = 2^{103}$.

References

[1] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff Jr., *Factorizations of $b_n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ Up to High Powers*, 3rd Edn., American Mathematical Society. Free on the Web—search for "Cunningham Project".

[2] Richard Crandall and Carl Pomerance, *Prime Numbers: A Computational Perspective*, Springer–Verlag 2000.

[3] Ian Stewart and David Tall, *Algebraic Numbewr Theory*, Chapman & Hall 1987.