NIEUW ARCHIEF
VOOR WISKUNDE Vierde serie Deel 14 No. 3 november 1996, pp. 375 – 389

Historical Background of the Number Field Sieve Factoring Method

R.-M. Elkenbracht-Huizing
CWI
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
e-mail: marije@cwi.nl

In this article we give a concise history of factoring, thereby concentrating on ideas and methods which can be found in the Number Field Sieve method. For more information about the history of factoring or about other important methods like ECM, Pollard $p-1$, Pollard ρ and SQUFOF, we refer to [5], [30], [2], [16].

1. Euclid

One of the first persons concerning himself with primality and compositeness of natural numbers was Euclid. In his work 'Elements' [7], written in about 300 B.C., he gave in Book VII the following definitions:

> *An unit is that by virtue of which each of the things that exist is called one.*
>
> *A prime number is that which is measured (= divided) by an unit alone.*
>
> *A composite number is that which is measured by some number.*

Although modern definitions are slightly different, it is clear that Euclid considered the same numbers being a unit, prime or composite among the natural numbers as we do today. In the same book he states in Proposition 30:

> *If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers.*

From this proposition one can deduce the Fundamental Theorem of Arithmetic, which states that factorization into primes is unique up to order.

2. Eratosthenes

The first algorithm which finds all primes up to a user-chosen bound n and which can also be used for factoring the numbers up to n, is due to Eratosthenes (276–194 B.C.). His 'Sieve of Eratosthenes' starts by listing all integers from 2 to n. Repeatedly the first number of the remaining list is prime, after which we cross off in the list all multiples of that prime. Because every composite number has a factor less than or equal to its square root, we can stop after we have found a prime larger than the square root of n. All remaining numbers in the list have to be prime. The strength of the Sieve of Eratosthenes is that it requires no expensive multiplications or divisions. This idea is also used in the Number Field Sieve.

The simplest algorithm to factor a given number is the 'trial division' method, which is still in use for finding prime divisors up to approximately six or seven decimal digits. It tries to divide a number by the primes which are in a prepared table or by $2, 3$ and subsequently by the terms of a sequence which contains the primes $5, 7, \ldots$ as a subsequence (like the numbers $6k \pm 1$). To find larger divisors, faster, less memory consuming methods are known at present; they will be discussed further on.

3. Fermat

In 1643 Fermat [8] noted that when n is composite and odd, then $n = xy$ with x, y odd and $1 < x \leq \sqrt{n}$. With $a = (x+y)/2$, $b = (x-y)/2$, we can deduce $n = a^2 - b^2$ and $\sqrt{n} \leq a < (n+1)/2$. Thus to factor n, one can consider all values of $r_i = a_i^2 - n$ for $a_0 = \lceil \sqrt{n} \rceil, a_1 = a_0 + 1, \ldots, a_{i+1} = a_i + 1, \ldots$ until r_i is a perfect square. Such an r_i does exist and $(a_i + \sqrt{r_i})(a_i - \sqrt{r_i})$ will be a non-trivial factorization of n. As Fermat noticed, his method can be made faster by calculating r_{i+1} from $r_{i+1} = r_i + 2a_i + 1$ and by using that for example a number ending on 19 cannot be a square. In an example Fermat factored $2027651281 = 44021 \cdot 46061$. If one knows that the factors of a composite number n are very close to $\sqrt{n}$ this method can still be used, otherwise for large n it is very ineffective. But the idea of constructing integers a^2 and b^2 such that n equals or – as used first in 1886 by Seelhoff [26] – more generally *divides* their difference, is used in many factoring methods, including the Number Field Sieve. Until 1886 however, most effort was spent in another direction.

4. Legendre

In his – originally published in 1798 – 'Théorie des Nombres' [11] Legendre gave a method to exclude more and more primes from being a possible divisor of n by finding more and more independent quadratic residues modulo n. If $x^2 \equiv a \bmod n$ has a solution x for a certain a, then a is a quadratic residue modulo n (denoted with the Legendre symbol $\left(\frac{a}{n}\right) = 1$) and a is also a quadratic residue for any prime divisor p of n. Since a is quadratic residue of only about half of the primes, this excludes the other primes as a possible divisor of n. If one has found k independent quadratic residues, the number of trial divisions of n can be reduced to about $2^{-k}\pi(\sqrt{n})$. Legendre finds quadratic residues modulo n by calculating continued fraction expansions of the square root of n and small multiples of n. Such expansions

$$\sqrt{kn} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}} \tag{1}$$

are denoted by $\sqrt{kn} = [c_0, c_1, c_2, c_3, \ldots]$ and can be calculated by defining $x_0 = \sqrt{kn}, c_i = \lfloor x_i \rfloor, x_{i+1} = 1/(x_i - c_i)$. They are infinite and periodic (see for example [24]). To calculate the partial denominators c_i we look at the example given by Legendre. He tried to factor the number $n = 333667$ by calculating the continued fraction expansion of $\sqrt{n}$ for which $x_0 = \sqrt{333667}$, $c_0 = 577$ and

$$\begin{array}{rclclcl}
x_1 & = & \frac{1}{\sqrt{n}-577} & = & \frac{\sqrt{n}+577}{738} & = & 1+\frac{\sqrt{n}-161}{738} \\
x_2 & = & \frac{738}{\sqrt{n}-161} & = & \frac{\sqrt{n}+161}{417} & = & 1+\frac{\sqrt{n}-256}{417} \\
x_3 & = & \frac{417}{\sqrt{n}-256} & = & \frac{\sqrt{n}+256}{643} & = & 1+\frac{\sqrt{n}-387}{643} \\
x_4 & = & \frac{643}{\sqrt{n}-387} & = & \frac{\sqrt{n}+387}{286} & = & 3+\frac{\sqrt{n}-471}{286} \quad \ldots
\end{array}$$

which gives $\sqrt{333667} = [577, 1, 1, 1, 3, \ldots]$. If we define Q_i by the denominator when we have written x_i in the form $(\sqrt{kn} + J)/Q_i$ then for certain a_i and b_i the equation

$$knb_i^2 = a_i^2 + (-1)^{i+1} Q_i \tag{2}$$

holds, which means that $(-1)^i Q_i$ is a quadratic residue modulo n. The a_i and b_i are the numerator and the denominator of the good (and in certain sense the best) rational approximation of $\sqrt{n}$ obtained by stopping the expansion (1) after c_i. They can also be calculated using the following sequences:

$$\left.\begin{array}{lll}
a_{-1} = 0, & a_0 = 1, & a_k = c_{k-1}a_{k-1} + a_{k-2} \\
b_{-1} = 1, & b_0 = 0, & b_k = c_{k-1}b_{k-1} + b_{k-2}
\end{array}\right\} k = 1, 2, \ldots$$

Thus Legendre found -738 (hence also -82), 417, -643, and (by expanding $\sqrt{n}$ further) also 69, -288 (hence also -2) as quadratic residues of n. The equality $3n = 1001001 = (1001)^2 - 10(10^2)$ gave him also 10 as quadratic residues of n. By using that the only primes p for which $\left(\frac{-2}{p}\right) = 1$ are of the form $8m + 1$ or $8m + 3$ and by using similar formulas for the restrictions $\left(\frac{10}{p}\right) = 1$, $\left(\frac{69}{p}\right) = 1$ and $\left(\frac{-82}{p}\right) = 1$, Legendre found that the only primes which could divide n are $83, 107, 163, 401, 409, 467$ and 569. None of them does divide n and therefore 333667 is prime. As we will see these ideas of Legendre are the basis of the modern factoring method CFRAC.

5. Gauss

A few years later, in 1801, Gauss indicated in his famous book 'Disquisitiones Arithmeticae' [9, Art. 329–332] that he was especially interested in small quadratic residues, so that he could use his prepared table in which he had denoted for all primes up to some bound whether or not they are a quadratic residue modulo small numbers. Note that if $\left(\frac{a}{n}\right) = 1$ and $\left(\frac{b}{n}\right) = 1$ then $\left(\frac{ab}{n}\right) = 1$ and if $\left(\frac{ak^2}{n}\right) = 1$, then $\left(\frac{a}{n}\right) = 1$. Therefore by finding many quadratic residues which factor over small primes, it is sometimes possible to construct *small* quadratic residues. Of the three methods to find quadratic residues that Gauss described, the simplest method writes a multiple of n as a sum: $kn = a + b$ where b can be negative. Now $-ab \equiv a^2 \bmod n$ is a quadratic residue modulo n. By taking for a (a small multiple of) a square differing from kn by a number that factors into small primes, one finds a useful quadratic residue. For example $n = 997331 = 2 \cdot 706^2 + 3 \cdot 17 \cdot 3^2$ gives $-2 \cdot 3 \cdot 17$ as a quadratic residue. Combining this with $3 \cdot 7 \cdot 17$ and 17 which he found with one of his other methods, gave -14 and -6. After finding that $-6, 13, -14, 17, 37$ and -53 are quadratic residues modulo 997331, Gauss consulted his prepared table of which we show here a small part with only the columns of the mentioned quadratic residues:

	−6	13	−14	17	37	−53
3	+	+	+		+	+
5	+		+			
7	+		+		+	
11	+				+	
⋮						
127	+	+	+	+	+	+
⋮						

It appears that 127 is the only prime $< \sqrt{n}$ for which $-6, 13, -14, 17, 37$ and -53 are all quadratic residues, and therefore the only candidate for being a divisor of n. Indeed $n = 127 \cdot 7853$. Further on we will return to this idea of trying to find and combine numbers which factor into small primes.

6. Sieving devices

Another important idea of Gauss [9, Art. 320] is nowadays called modular exclusion. He wanted to solve the equation $x^2 = a + my$, for integers x and y, but his observation applies to $f(x) = g(y)$ for $f(x), g(x) \in \mathbb{Z}[x]$. Select different moduli $E_1, E_2, \ldots E_r$ and find for each value of $x = 0, 1, \ldots E_i$ the possible residue classes for y modulo E_i. Combine these to find the permissible residue classes for y modulo the least common multiple of the E_i's. This idea was used for factoring numbers of the form $(a^k - 1)/(a - 1)$ by Pepin [21]. He found that an equation of the form

$$az^2 + 2bz + c = u^2 \tag{3}$$

where a, b and c are known integers and the value of z is bounded (in terms of a, b, c), should have a solution for z and u. With help of the modular exclusion technique of Gauss he tried to find solutions. LAWRENCE [10] was the first who had the idea of building a machine for mechanizing the process of solving (3). As described in [30]:

> "Lawrence suggested the construction of a machine in which gears of m teeth would be used for each exclusion modulus m. The gears (each with the same tooth size) would be driven by the same diving gear, and, as they would be of differing diameters, would have to be mounted on different shafts. The teeth on each m-toothed gear would be numbered $0, 1, 2, \ldots, m-1$, and a brass stud would penetrate through it at the point(s) of an acceptable (mod m) residue (One for which (3) could hold for $z \bmod m$). When studs from each of the gears were all in contact a circuit would be completed and a bell would ring or the machine would stop, indicating to the operator that a solution of (3), modulo the least common multiple of the exclusion moduli, had been detected. Of course, in order to determine the z-value, a count would have to be recorded of the number of rotations of the driving gear."

As can be read in [30], [29], [14] and [20] many persons, the most prominent being Lehmer, have actually built these kind of machines and factored numbers with them. Up to 1970 these sieve methods were the fastest techniques for factoring.

7. SEELHOFF

In 1886 SEELHOFF [26] published a method in which he used the ideas of Fermat and Gauss. Put $n = \omega^2 + r$, where $\omega = \lfloor\sqrt{n}\rfloor$. If p is any prime such that $\left(\frac{n}{p}\right) = 1$, solve $\rho^2 \equiv n \bmod p^k$. Seelhoff suggested that for values of n of approximately 15 digits, one could try for p^k: $p = 2$ with $k \leq 10$, 3 with $k \leq 6$, 5 with $k \leq 4$ and the primes from 7 to 97 with $k \leq 2$. Try to find a y such that $b = \alpha(2\omega - \alpha) + r$ where $\alpha = \omega + (\rho + yp^k)$ factors into a square and small primes. We then have $n = (\omega - \alpha)^2 + b$ and $p^k | b$. When $|\alpha|$ is near p^k, then $|b|$ will be approximately $2p^k\sqrt{n}$. Because b is divisible by p^k, b should be much easier to factor than n. One hopes to find a selection of the equalities $(\omega - \alpha)^2 = -b + n$ such that the multiplication of their various $-b$'s gives a square.

As an illustration of this method we give Seelhoff's example. For $n = 7 \cdot 2^{34} + 1$ we get $\omega = 346783$ and $r = 635200$. He found three solutions of $\rho^2 \equiv n \bmod p^k$ and values of a, such that b factored in a square times small primes:

$\rho^2 \equiv n \bmod p^k$	α	b	$(\omega-\alpha)^2 = -b+n$
$155^2 \equiv n \bmod 37^2$	1950	$2 \cdot 7 \cdot 11 \cdot 2960^2$	$344833^2 = -2 \cdot 7 \cdot 11 \cdot 2960^2 + n$
$6326^2 \equiv n \bmod 127^2$	143432	$7 \cdot 106172^2$	$203351^2 = -7 \cdot 106172^2 + n$
$1214^2 \equiv n \bmod 37^2$	-3836	$-2 \cdot 11 \cdot 11026^2$	$350619^2 = 2 \cdot 11 \cdot 11026^2 + n$

From the first two equations he obtained:

$$11 \cdot 832082029^2 \equiv 2 \cdot 150479740^2 \bmod n$$

and combining this result with the third equation gave:

$$50459950484647^2 \equiv 26380527979530^2 \bmod n$$

or

$n \mid (50459950484647 - 26380527979530) \times (50459950484647 + 26380527979530)$.

Now $\gcd(50459950484647 - 26380527979530, n) = 317306291$ gives a factor of n. Thus Seelhoff - as can be read in [30] - and not Kraitchik as for example stated in [24], was the first who combined congruences consisting of squares and small primes modulo n to an equation of the form $a^2 \equiv b^2 \bmod n$.

8. Lehmer and Powers

From the way Seelhoff used his equations $(\omega - \alpha)^2 = -b + n$ one can deduce that the only thing one really needs are congruences of the form $a^2 \equiv b \bmod n$ such that the product of the b's is a square. It was noted by Lehmer and Powers [12] that one can use equation (2) to construct these kind of congruences. If we define $R_i := (-1)^i Q_i$, then equation (2) gives the congruence

$$a_i^2 \equiv R_i \bmod n.$$

When $\{R_{i_1}, R_{i_2}, \ldots, R_{i_k}\}$ is a subset of the R_i's such that their product is R^2, then we have

$$\left(\prod_{j=1}^{k} a_{i_j} \right)^2 \equiv R^2 \bmod n.$$

If n is odd and not a prime(power), calculating the greatest common divisor of $\prod_{j=1}^{k} a_{i_j} - R$ and n gives a factor of n for at least half of the solutions of $x^2 \equiv y^2 \bmod n$ with $y \not\equiv 0 \bmod n$. Because of the tedious calculations to find an appropriate subset, which often gave a trivial factorization, Lehmer and Powers did not consider their method to be practical. It was however the basis for the Continued Fraction method of Morrison and Brillhart.

9. Morrison and Brillhart

In 1970 Morrison and Brillhart [18] developed the Continued Fraction method (CFRAC), by combining the idea of Lehmer and Powers with a method to construct R from a set of 'promising' R_i's. With their method they set a new record by factoring F_7, the seventh Fermat number of 39 digits [19]. They introduced the 'factor base', a collection $\mathcal{F}(B)$ of primes up to a certain bound B, and searched for R_i's which factor completely over these primes. Since by (2) primes p for which $\left(\frac{kn}{p}\right) = -1$ will never appear in the factorization of

R_i's, they defined $\mathcal{F}(B)$ as the set of primes p up to B with $\left(\frac{kn}{p}\right) \geq 0$. If an R_i factors completely over $\mathcal{F}(B)$ we can write

$$R_i = (-1)^{e(i,-1)} \prod_{p \in \mathcal{F}(B)} p^{e(i,p)}$$

and call R_i a relation. In order that the product over a subset $\mathcal{S}$ of the relations is a square, every exponent $\sum_{\mathcal{S}} e(i,s)$ in

$$\prod_{R_i \in \mathcal{S}} R_i = (-1)^{\sum_{\mathcal{S}} e(i,-1)} \prod_{p \in \mathcal{F}(B)} p^{\sum_{\mathcal{S}} e(i,p)} = R^2 \tag{4}$$

should be even. For every R_i which factors completely over the factor base, Morrison and Brillhart defined a vector $\boldsymbol{v}(i)$ of length $1 + |\mathcal{F}(b)|$. This vector contains all $e(i,s) \bmod 2$ – indicating if s occurs in R_i to an even or an odd power – in an order which is the same for all R_i's. The vectors are put as columns in a matrix, and a non-trivial vector of the null space over $\mathbb{F}_2$ of this matrix indicates a subset $\mathcal{S}$ for which (4) holds.

As an example Morrison and Brillhart factored the number $n = 13290059$. By expanding $\sqrt{n}$ and by using trial division they found the following R_i's which factor completely over the primes in $\mathcal{F}(113)$:

i	$a_i \bmod n$	R_i factored
5	171341	$-1 \cdot 2 \cdot 5^2 \cdot 41$
10	6700527	$31 \cdot 43$
22	5235158	$41 \cdot 113$
23	1914221	$-1 \cdot 2 \cdot 113$
26	11455708	$2 \cdot 31 \cdot 53$
31	1895246	$-1 \cdot 2 \cdot 5^2 \cdot 113$
40	3213960	$2 \cdot 43 \cdot 53$

Subsequently a matrix is formed by taking as columns the vectors $\boldsymbol{v}(i)$. Here we only show the rows corresponding to the factors which occur in the factorizations of the above stated R_i's:

$$\begin{array}{r@{\quad}l}
 & \begin{array}{ccccccc} \boldsymbol{v}(5) & \boldsymbol{v}(10) & \boldsymbol{v}(22) & \boldsymbol{v}(23) & \boldsymbol{v}(26) & \boldsymbol{v}(31) & \boldsymbol{v}(40) \end{array} \\
\begin{array}{r} -1 \\ 2 \\ 5 \\ 31 \\ 41 \\ 43 \\ 53 \\ 113 \end{array} &
\left(\begin{array}{ccccccc}
1 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 0
\end{array}\right)
\end{array}$$

Using Gaussian elimination over $\mathbb{F}_2$, Morrison and Brillhart found that the three vectors $(0,1,0,0,1,0,1)^t$, $(1,0,1,0,0,1,0)^t$ and $(1,0,1,1,0,0,0)^t$ are in the kernel of this matrix. The first vector corresponds with $\mathcal{S} = \{R_{10}, R_{26}, R_{40}\}$ and gives the congruence

$$(6700527 \cdot 11455708 \cdot 3213960)^2 \equiv (2 \cdot 31 \cdot 43 \cdot 53)^2 \bmod n$$

or $141298^2 \equiv 141298^2 \bmod n$, which does not give a factorization of n. From the second vector we can deduce

$$(171341 \cdot 5235158 \cdot 1895246)^2 \equiv (2 \cdot 5^2 \cdot 41 \cdot 113)^2 \bmod n,$$

what reduces to $13058409^2 \equiv 231650^2 \bmod n$. But $\gcd(13058409-231650, n) = 1$ and this dependency fails also to give a non-trivial factorization of n. Finally the last vector leads via

$$(171341 \cdot 5235158 \cdot 1914221)^2 \equiv (2 \cdot 5 \cdot 41 \cdot 113)^2 \bmod n$$

and $1469504^2 \equiv 46330^2 \bmod n$ to the factor $\gcd(1469504-46330, n) = 4261$ of n.

Morrison and Brillhart also introduced a refinement of the factor base approach, which cuts the total running time by almost one half. They used what had been previously noticed by Eratosthenes: if one has removed all prime divisors up to a bound B from a number r, and the remaining cofactor is less than B^2, then the cofactor is prime. Now also R_i's which – after removing the factors up to B with trial division – have a remaining (prime) cofactor between B and B^2 are used as relation. Because these relations factor over $\mathcal{F}(B^2)$ instead of over $\mathcal{F}(B)$, the vectors $\boldsymbol{v}(i)$ should be of length $1+|\mathcal{F}(B^2)|$ and contain the values of $e(i,s)$ for all factors $s < B^2$. The corresponding matrix will have more rows and therefore, to guarantee the existence of non-trivial vectors in the kernel, also more relations have to be found. But the increase in efficiency of finding relations is so large, that the net result is positive. Morrison and Brillhart spent up to 95% of the computer time on the trial divisions. With use of computers the method defeated the sieving devices and reigned until the introduction in 1982 of the Quadratic Sieve method, in which the trial divisions are replaced by sieving. Before we discuss this method, we describe the discovery of the so-called RSA cryptosystem.

10. Rivest, Shamir and Adleman

In 1977 Rivest, Shamir and Adleman introduced the RSA public-key cryptosystem [25]. Together with the increase of computing power, this application of the supposed difficulty of factoring was an enormous stimulus for the interest in and development of factoring methods. The idea of a public-key cryptosystem, where each user u has his own encryption and decryption procedure, was introduced in 1976 by Diffie and Hellman [6]. The encryption procedure E_u is placed in a public file and other persons can use this procedure to encrypt their message M and send the resulting cipher-text $E_u(M)$ to the user. Only the user u has the corresponding secret decryption procedure D_u, which he can apply to reveal the original message $M = D_u(E_u(M))$. Besides encryption a public-key cryptosystem can also be used to sign a message. User u can sign a message M by sending $D_u(M)$. Anyone can apply the publicly known encryption procedure E_u of the user to reveal $M = E_u(D_u(M))$ and concludes that only user u himself could have constructed $D_u(M)$. The procedures D and E must be bijections and inverses of each other: $D(E(M) = E(D(M)) = M$ for all M. Furthermore both $D(M)$ and $E(M)$ should be quickly to compute, pairs (D, E) should be easy to construct and it should be computationally infeasible to find D given E.

RSA achieves these objectives by letting each user pick two large primes p and q with $p \neq q$. Furthermore it chooses two exponents d and e with $de \equiv 1 \bmod (p-1)(q-1)$. With $n = pq$ the encryption procedure is defined by $E(M) = M^e \bmod n$ and the decryption procedure by $D(M) = M^d \bmod n$. The values of e and n are public, but d, p and q are private. With Euler's theorem one can prove that $D(E(M) = E(D(M)) = M$ for all M. The safety of this cryptosystem is supposed to be as difficult as factoring. When one can find p and q from n, together with e, one can deduce d.

Rivest, Shamir and Adleman encrypted as an example the sentence "its all greek to me" (Julius Caesar). With $p = 47$, $q = 59$ and $n = pq = 2773$ they computed (with a variation of Euclid's greatest common divisor algorithm) $e = 17$ and $d = 157$. With $n = 2773$ they encoded two letters at a time, substituting a two-digit number for each letter: blank$= 00, a = 01, b = 02, \ldots, z = 26$. Thus the message

its all greek to me

is replaced by the numbers

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500.

To encrypt this message every number of 4 digits is raised to the 17th power and taken modulo n. For example $920^{17} \equiv 948 \bmod n$. Thus the whole message is enciphered as:

0948 2342 1084 1444 2663 2390 0778 0774 0219 1655.

With deciphering, like $948^{157} \equiv 920 \bmod n$ the original numbers can be revealed.

11. Pomerance

In 1982 Pomerance published the Quadratic Sieve method [23], in which most of the time-consuming trial divisions of the CFRAC method have been replaced by – for a computer much cheaper – additions. He found congruences modulo n by searching for values of x for which $f(x) = x^2 - n$ factors over the factor base. These values are found by initializing an array with $|f(x)|$ for a range of consecutive x-values ($\sqrt{n} - M \leq x \leq \sqrt{n} + M$, say) and by dividing these $|f(x)|$-values by all primes in $\mathcal{F}(B)$ in a cheap way. Note that if $f(x) \in \mathbb{Z}[x]$, and $p | f(x_0)$ for some x_0, than $p | f(x_0 + kp)$ $\forall k \in \mathbb{Z}$. For every root $f(r) \equiv 0 \bmod p$ one constructs the smallest $t \equiv r \bmod p$ in the array and divides p from all

$|f(t+kp)|$ for $0 \le k \le \lfloor(\sqrt{n}+M-t)/p\rfloor$. When this is done for all roots and all $p \in \mathcal{F}(B)$, the array elements containing 1 betray that the corresponding $f(x)$ factors over the primes and that a relation is found. To find the factorization of $f(x)$ trial division should be applied, but note that we apply it to the relations only, which is a very small part of all investigated $f(x)$ values. A refinement of this method was proposed by Davis and Holdridge and applied to factor several numbers in the range of 53–71 digits [4].

If we sieve the $2M$ values for $\sqrt{n}-M \le x \le \sqrt{n}+M$, then the largest residue is about $2M\sqrt{n}$ (assuming $M \ll n$). MONTGOMERY [28] found a way to stunt this growth as M grows. His Multiple Polynomial Quadratic Sieve (MPQS) method finds many polynomials $f(x) = a^2x^2 + bx + c$ with $b^2 - 4a^2c = kn$. Note that

$$f(x) = \left(ax + \frac{b}{2a}\right)^2 - \frac{b^2 - 4a^2c}{4a^2} \equiv \left(ax + \frac{b}{2a}\right)^2 \bmod n.$$

The values of a, b and c are selected such that when sieving over an interval $|x| \le M_0$ the largest residue is at most $M_0\sqrt{n/2}$. To sieve $2M$ values of x, one can use M/M_0 different polynomials, sieving $2M_0$ values per polynomial with largest residual $M_0\sqrt{n/2}$. The reduction of $2M\sqrt{n}$ to the much smaller $M_0\sqrt{n/2}$ is important, since small numbers are more likely to have all prime factors in $\mathcal{F}(B)$.

The sieving procedure can be speeded up in several ways. One can initialize the array with log $|f(x)|$ instead of $|f(x)|$ and subtract [log p] (where [.] is the nearest integer function) instead of dividing by p. One can use rounded logarithms to work with integers instead of reals. For an optimal balance between precision and efficiency one can use a base such that the maximum value of $|f(x)|$ just fits in one byte. Sieving over small primes is a lot of work and just a small amount of [log p] is added. Therefore it is more efficient to sieve over a power of the small primes (< 30, say) only. All these adjustments do not only make the sieving faster, but also make the final value in the array elements less accurate. After sieving one should check if the remaining value looks 'promising', i.e. is smaller than some user-determined bound c. For these 'candidate relations' one can use trial division to investigate if they really factor over $\mathcal{F}(B)$. In the 'large prime variation' one also wants to find relations containing one large prime q (with $B < q \le L < B^2$) and therefore adds log L to c. There exists even a 'double large prime variation' where one adds 2 log L to c and tries to factor (with for example SQUFOF [27], [24, p. 186–193], [2, §8.7]) a remaining cofactor $\le L^2$ into at most two prime factors $< L$. This version was used in 1994 by A.K. Lenstra and Atkins and 600 volunteers when they factored the so-called RSA-129, a number that had been given in 1977 by Rivest, Shamir and Adleman to challenge computer scientists [1]. All these ideas can be applied in the Number Field Sieve method as well, the original version of which was discovered by John Pollard.

12. Pollard

The Special Number Field Sieve (SNFS) method, introduced in 1988 by POLLARD [22] and developed in [13], is nowadays the fastest method for numbers of the form $c_1r^t + c_2s^u$. The world record is the factorization of $(12^{151} - 1)/11$, a number of 162 decimal digits, which was established in 1994 by Oregon State University, Oregon, USA and CWI, Amsterdam, The Netherlands. Already in [13] attempts were made to extend the method to arbitrary integers. Nowadays the General Number Field Sieve (GNFS) method is much more developed and it beats the MPQS method for numbers of more than approximately 105 decimal digits.

The NFS method consists of five stages. In the first stage two irreducible polynomials $f(x), g(x) \in \mathbb{Z}[x]$ and an integer m are selected, such that $f(m) \equiv g(m) \equiv 0 \bmod n$. Often one takes $f(x) = x - m$ and for $g(x)$ the base-m expansion of n, for suitable m. The smaller the coefficients are, the faster the method is. When applying SNFS, one can use the special form of the number and find very small coefficients for one of the polynomials. This makes SNFS considerably faster than GNFS. For simplicity we consider $f(x)$ and $g(x)$ to be monic in the rest of this chapter.

Let α be a root of f and β of g. In the sieving stage we find relations (a, b) with $\gcd(a, b) = 1$ such that the integral norms of $a - b\alpha$ and $a - b\beta$

$$N(a - b\alpha) = b^{\deg(f)} f(a/b) \quad \text{and} \quad N(a - b\beta) = b^{\deg(g)} g(a/b)$$

factor over a factor base $\mathcal{F}(B)$. This is done, similar to the MPQS method, by initializing for each value of b and for a range of a-values, an array, first with the values of $\log |N(a - b\alpha)|$ followed by the values of $\log |N(a - b\beta)|$. For values of a for which both residues look promising, $N(a - b\alpha)$ and $N(a - b\beta)$ can be investigated further with trial division. Although we require two values to be smooth – instead of only one value in MPQS –, the values of $N(a - b\alpha)$ and $N(a - b\beta)$ are so much smaller that there is an overall gain. In fact one sieves for pairs (a, b) such that both ideals $(a - b\alpha)\mathcal{O}_\alpha$ and $(a - b\beta)\mathcal{O}_\beta$ factor over prime ideals with norm $< B$.

In the filtering stage we try to reduce the size of the matrix. If a prime ideal is occurring only once to an odd power, the corresponding relation is thrown away. If a prime ideal is occurring twice to an odd power, the two relations are grouped and the prime ideal will disappear from the matrix.

Denote by $\mathbb{Q}_n$ the ring of rational numbers with denominator coprime to n. The subring $\mathbb{Q}_n[\alpha]$ of $\mathbb{Q}(\alpha)$ consists of expressions $\sum_{i=0}^{deg(f)-1} (s_i/t_i)\alpha^i$ with $s_i, t_i \in \mathbb{Z}$ and $\gcd(n, t_i) = 1$. In the linear algebra stage a matrix is built such that a vector of the kernel corresponds with a subset $\mathcal{S}$ of the relations for which both $\prod_{\mathcal{S}}(a - b\alpha)$ and $\prod_{\mathcal{S}}(a - b\beta)$ are squares – say γ^2 and δ^2 – in $\mathbb{Q}_n[\alpha]$ and $\mathbb{Q}_n[\beta]$, respectively. Among other requirements $\mathcal{S}$ is constructed such that all occurring prime ideals occur to an even power.

The final square root stage serves to construct γ and δ from the found γ^2 and δ^2. Thus we have to extract two square roots in algebraic number fields. Having obtained γ and δ one constructs a quadratic congruence modulo n in the following way: Define two natural ring homomorphisms:

$\phi_\alpha : \mathbb{Q}_n[\alpha] \to \mathbb{Z}/n\mathbb{Z}$ and $\phi_\beta : \mathbb{Q}_n[\beta] \to \mathbb{Z}/n\mathbb{Z}$ by $\phi_\alpha(\alpha) = \phi_\beta(\beta) = m \bmod n$. Thus $\phi_\alpha(\sum_{i=0}^{deg(f)-1}(s_i/t_i)\alpha^i) = (\sum_{i=0}^{deg(f)-1} s_i t_i^{-1} m^i \bmod n)$ for $s_i, t_i \in \mathbb{Z}$ and $\gcd(n, t_i) = 1$. When $\phi_\alpha(\gamma) = c \bmod n$ and $\phi_\beta(\delta) = d \bmod n$, we have

$$c^2 \overset{n}{=} \{\phi_\alpha(\gamma)\}^2 = \phi_\alpha(\gamma^2) = \phi_\alpha(\prod_{(a,b)\in\mathcal{S}} (a - b\alpha)) \overset{n}{=} \prod_{(a,b)\in\mathcal{S}} (a - bm) \overset{n}{=}$$

$$\phi_\beta(\prod_{(a,b)\in\mathcal{S}} (a - b\beta)) = \phi_\beta(\delta^2) = \{\phi_\beta(\delta)\}^2 \overset{n}{=} d^2,$$

where $\overset{n}{=}$ means equality modulo n.

Montgomery, who has done important work in developing the NFS method ([17], [15]) gives an example of this method in [16]. Using CWI's address, he picks the number 1098413 and applies SNFS by noticing that $1098413 = 12 \cdot 45^3 + 17^3$. With $m = \frac{17}{45}$, he uses

$$\begin{array}{ll} f(x) = x^3 + 12 & (f(m) = \left(\frac{17}{45}\right)^3 + 12 \equiv 0 \bmod n) \\ g(x) = 45x - 17 & (g(m) = 45\left(\frac{17}{45}\right) - 17 \equiv 0 \bmod n) \end{array}$$

For these polynomials we find the following set $\mathcal{S} = \{(6,1), (-3,2), (7,3), (-1,3), (2,5), (3,8), (-9,10)\}$. With $\alpha = \sqrt[3]{-12}$ and $\beta = \frac{17}{45}$ one can deduce:

$$\begin{aligned} \prod_{\mathcal{S}}(a - b\alpha) &= 7400772 + 1138236\alpha - 105495\alpha^2 \\ &= (2694 + 213\alpha - 28\alpha^2)^2 = \gamma^2 \\ \prod_{\mathcal{S}}(a - b\beta) &= \frac{2^8 \cdot 11^2 \cdot 13^2 \cdot 23^2}{3^{12} \cdot 5^4} = \left(\frac{52624}{18225}\right)^2. \end{aligned}$$

Because $\phi_\alpha(\gamma) = \frac{5610203}{2025} \bmod n$, Montgomery gets the congruence

$$\left(\frac{52624}{18225}\right)^2 \equiv \left(\frac{5610203}{2025}\right)^2 \bmod n$$

and $\gcd(52624 \cdot 2025 - 5610203 \cdot 18225, n) = 1951$ gives the factor 1951 of 1098413.

13. RSA130

On April 10, 1996 a new world record was set by the factorization of RSA130, a number (not having a special form) of 130 decimal digits [3]. An international team under guidance of A.K. Lenstra used the General Number Field Sieve method to beat the 129-digit record that was set on April 2, 1994 by the Quadratic Sieve method. The gathering of the needed $56 \cdot 10^6$ relations would have taken 16.5 years on a Sparc 10 workstation with 24 megabytes available for the sieving process. However, with the help of the World Wide Web many people could contribute and the sieving phase was done in a few months. The filtering stage resulted in a 3516502 × 3504823 matrix over $\mathbb{F}_2$. Using the 'block Lanczos method' [17] it took 67.5 CPU-hours and 700 megabytes central memory on a Cray C-90 supercomputer to find 18 vectors of the kernel. The first two vectors gave trivial factorizations, but the third vector produced:

RSA130 =
18070 82088 68740 48059 51656 16440 59055 66278 10251 67694 01349 17012 70214
50056 66254 02440 48387 34112 75908 12303 37178 18879 66563 18201 32148 80557
=
39685 99945 95974 54290 16112 61628 83786 06757 64491 12810 06483 25551 57243
×
45534 49864 67359 72188 40368 68972 74408 86435 63012 63205 06960 09990 44599

ACKNOWLEDGEMENTS
The author thanks H.J.J. te Riele and R. Tijdeman for reading the paper and for suggesting several improvements.

REFERENCES

1. D. ATKINS, M. GRAFF, A.K. LENSTRA, AND P.C. LEYLAND, 1995, The magic words are squeamish ossifrage. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology - Asiacrypt '94*, volume 917 of *Lecture Notes in Computer Science*, pages 265–277, Springer–Verlag, Berlin.
2. H. COHEN, 1993, *A Course in Computational Algebraic Number Theory.* Springer–Verlag, Berlin.
3. J. COWIE, B. DODSON, R.-M. ELKENBRACHT-HUIZING, A.K. LENSTRA, P.L. MONTGOMERY AND J. ZAYER. A world wide number field sieve factoring record: on to 512 bits. In *Advances in Cryptology - Asiacrypt '96*, Lecture Notes in Computer Science. To appear.
4. J.A. DAVIS, D.B. HOLDRIDGE, AND G.J. SIMMONS, 1985, Status report on factoring (at the Sandia National Laboratories). In T. Beth, N. Cot and I. Ingemarsson, editors, *Advances in Cryptology - EUROCRYPT '84*, volume 209 of *Lecture Notes in Computer Science*, pages 183–215, Springer–Verlag, Berlin.
5. L.E. DICKSON, 1934, *History of the theory of numbers.* Carnegie Institution of Washington, Washington, 1919–1920. Reprint: Stechert, New York.
6. W. DIFFIE AND M. HELLMAN, 1976, New directions in cryptography. *IEEE Trans. Inform. Theory IT-22*, 6:644–654.
7. EUCLID, 1926, *The thirteen books of Euclid's Elements.* Cambridge University Press, Cambridge, 2nd edition. Translated with introduction and commentary by J.L. Heiberg and T. L. Heath. Reprint: Dover publications, inc., New York, 1956.
8. P. DE FERMAT, 1894, In P. Tannery and C. Henry, editors, *Oeuvres de Fermat*, volume 2, pages 256–258. Gauthier–Villars et fils, Paris. Fragment of a letter of about 1643 to Mersenne or to Frenicle.
9. C.F. GAUSS, 1966, *Disquisitiones Arithmeticae.* Yale University Press, New Haven and London. Originally published in 1801.

10. F.W. LAWRENCE, 1896, Factorisation of numbers. *Quarterly Journal oj Pure and Applied Mathematics*, 28:285–311.
11. A.-M. LEGENDRE, 1893, *Zahlentheorie*, volume 1, pages 331–336. B.G. Teubner, Leipzig. Originally published as 'Théorie des nombres' in 1798.
12. D.H. LEHMER AND R.E. POWERS, 1931, On factoring large numbers. *Bulletin of the American Mathematical Society*, 37:770–776.
13. A.K. LENSTRA AND H.W. LENSTRA, JR., 1993, *The development of the number field sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer–Verlag, Berlin.
14. R.F. LUKES, C.D. PATTERSON AND H.C. WILLIAMS, 1995, Numerical Sieving Devices: Their History and Some Applications. *Nieuw Archief voor Wiskunde*, 13(1):113–139.
15. P.L. MONTGOMERY, 1994, Square roots of products of algebraic numbers. In W. Gautschi, editor, *Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics*, volume 48, pages 567–571. Proceedings of Symposia in Applied Mathematics, American Mathematical Society.
16. P.L. MONTGOMERY, 1994, A survey of modern integer factoring algorithms. *CWI Quarterly*, 7/4:337–366.
17. P.L. MONTGOMERY, 1995, A block Lanczos algorithm for finding dependencies over GF(2). In L.C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, volume 921 of *Lecture Notes in Computer Science*, pages 106–120, Springer–Verlag, Berlin.
18. M.A. MORRISON AND J. BRILLHART, 1975, A method of factoring and the factorization of F_7. *Mathematics of Computation*, 29:183–205.
19. M.A. MORRISON AND J. BRILLHART, 1971, The factorization of F_7. *Bulletin of the American Mathematical Society*, 77:264.
20. C. PATTERSON, 1991, *The derivation of a high speed sieve device.* PhD thesis, Department of Computer Science, University of Calgary, Calgary, Canada.
21. T. PEPIN, 1889–1890, Sur la décomposition des grandes nombres en facteurs premiers. *Atti della Accademia Pontificia dei Nuovi Lincei*, 43:163–191.
22. J.M. POLLARD. *Factoring with cubic integers*, pages 4–10 in [13].
23. C. POMERANCE, 1982, Analysis and comparison of some integer factoring algorithms. In H.W. Lenstra, Jr. and R. Tijdeman, editors, *Computational methods in number theory*, volume 154 of *Mathematical Centre Tracts*, pages 89–139. Mathematisch Centrum, Amsterdam.
24. H. RIESEL, 1994, *Prime Numbers and Computer Methods for Factorization.* Birkhäuser, Boston, 2nd edition.
25. R.L. RIVEST, A. SHAMIR AND L. ADLEMAN, 1978, A method for obtaining digital signatures and public-key cryptosystems. *Communications of the Association for Computing Machinery*, 21(2):120–126.
26. P. SEELHOFF, 1886, Die Auflösung grosser Zahlen in ihre Factoren. *Zeitschrift für Mathematik und Physik*, 31:166–172. French translation in *Sphinx-Oedipe*, 7:84–88, 1912.

27. D. SHANKS, 1971, Class number, a theory of factorization, and genera. *American Mathematical Society Proceedings of Symposia in Pure Mathematics*, 20:415–440.

28. R.D. SILVERMAN, 1987, The multiple polynomial quadratic sieve. *Mathematics of Computation*, 48(177):329–339.

29. A.J. STEPHENS AND H.C. WILLIAMS, 1990, An open architecture number sieve. *London Mathematical Society Lecture Note Series*, 154:38–75.

30. H.C. WILLIAMS AND J.O. SHALLIT, 1994, Factoring integers before computers. In W. Gautschi, editor, *Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics*, volume 48, pages 481–531. Proceedings of Symposia in Applied Mathematics, American Mathematical Society.