LENSTRA'S FACTORISATION METHOD BASED ON ELLIPTIC CURVES

N.M.Stephens
University College
Cardiff
Great Britain

0. Introduction

The purpose of this exposition is to explain the method due to H.W.Lenstra, Jr. [1] of determining a non-trivial factor, p , of a composite number, n . The method uses the theory of elliptic curves and has an expected running time of $L(p)^{1/2}$ where $L(p)=\exp(\sqrt{\log p \log \log p})$. The aim of the exposition is to be completely elementary. It begins with an introduction to the arithmetic of elliptic curves sufficient to enable the reader to follow the later section explaining the method. The paper ends with a few remarks on techniques for the practical implementation of the algorithm.

The problem of finding efficient algorithms to decide whether or not a number is prime (primality testing) and to determine a non-trivial divisor of a composite number (factorisation) has a long history and has been considered by many number theorists including Fermat and Gauss. The more recent motivation for the study of the problem is the apparent security of the RSA public key cryptographic system based on the difficulty to factorise a number which is the product of two large primes.

The classical technique of trial division by all numbers up to $\sqrt{n}$ can be used to test the primality of n and to factor n . It has running time $O(\sqrt{n})$ which in terms of $\log n$ (the most reasonable measure of the size of the problem) is $O(\exp(c \log n))$ with $c=1/2$. Thus the trial division technique is said to have exponential running time.

Progress in the factorisation problem was made in the early 1970's. The methods still had exponential running time but the constant c was smaller. Lehman's method was with $c=1/3$; Shanks provably with $c=1/4$ but with $c=1/5$ assuming the extended Riemann Hypothesis; Pollard's rho method has an expected running time with $c=1/4$.

Newer advances were based on Fermat's idea that a non trivial solution of

$$x^2 \equiv y^2 \pmod{n}$$

yields a non-trivial factor of n , viz the highest common factor of $x-y$

and n . The determination of a solution and the analysis of the efficiency of the method required the concept of a "smooth" number (see later). The various methods exploiting this idea are difficult to analyse exactly but may reasonably be assumed to have sub-exponential running times. That is, to factorise n requires time $L(n)^Y$ for some constant Y , and similar storage requirements. The best value of Y so far achieved using these techniques is $Y=1$. In practice, the time to factor $n=pq$, where p and q are primes of size about 10^{30} , on a big machine is 28 hours [2].

1. Elliptic Curves

Let F be a field; for the purpose of this exposition, F may be assumed to be $\mathbb{Q}$, the rational numbers, or $\mathbb{F}_p$, the set of residues modulo a large prime p . An elliptic curve is an equation in x and y of the form

$$E: y^2 = x^3 + Ax + B$$

where A, B are integers such that $4A^3 + 27B^2 \neq 0$. (This is a technical condition which prevents the cubic in x having a linear factor squared.)

A point on the curve is either a pair (x, y) with $x, y \in F$ satisfying the equation or the pair $(\infty, \infty) = \underline{0}$. The set of all points $E(F)$ forms an abelian group. The zero of the group is $\underline{0}$. The negative of (x, y) is $(x, -y)$. The sum of $\underline{p}_1 = (x_1, y_1)$ and $\underline{p}_2 = (x_2, y_2)$ with $\underline{p}_1 \neq \underline{p}_2$ and $\underline{p}_1, \underline{p}_2 \neq \underline{0}$ is given as follows:

$$\text{let } m = \begin{cases} (y_2 - y_1) / (x_2 - x_1) & x_1 \neq x_2 \\ (3x_1^2 + A) / (2y_1) & x_1 = x_2 \end{cases}$$

Then $\underline{p}_1 + \underline{p}_2 = \underline{p}_3 = (x_3, y_3)$ is given by

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

One can check that with addition defined as above that $E(F)$ is indeed an abelian group, but some motivation for the formula would probably make the reader happier and less inclined to skip the rest of this article. The explanation is best illustrated with the field $F = \mathbb{R}$ the set of real numbers. The curve E can then be represented as in figure 1.

Figure 1

The line joining the points $\underline{P}_1$ and $\underline{P}_2$ has gradient m given by the above formula; the alternative is derived from the limiting case when the chord becomes the tangent at $\underline{P}_1$. This line intersects the curve at one further point $\underline{P}'$, whose negative is defined to be the sum of $\underline{P}_1$ and $\underline{P}_2$.

One way of interpreting the addition law on $E(F)$ is to state that the three points $\underline{P}$, $\underline{Q}$ and $\underline{R} \in E(F)$ are colinear if and only if

$$\underline{P} + \underline{Q} + \underline{R} = \underline{0}$$

Note that the addition law lends itself very easily to computation. If $M\underline{P}$ denotes the point $\underline{P}$ added to itself M times, then $M\underline{P}$ can be computed using the standard divide and conquer technique in $O(\log M)$ arithmetic steps.

Example To illustrate the addition law, consider the elliptic curve

$$E : y^2 = x^3 - 16x + 16 .$$

Over $\mathbb{Q}$, there is an obvious point $\underline{P} = (0, 4)$. To obtain $2\underline{P} = (0, 4) + (0, 4)$ we need to use the tangent formula for m :

$$m = (3x_1^2 + A)/(2y_1) = -2$$

from which we obtain $2\underline{P} = (4, 4)$. From $\underline{P}$ and $2\underline{P}$ we obtain $3\underline{P}$ by using the chord formula for m :

$$m = (y_2 - y_1)/(x_2 - x_1) = 0$$

and hence $3\underline{P} = (-4, -4)$. Continuing in this way, further multiples of $\underline{P}$ are:

$$4\underline{P} = (8, -20)$$

$$5\underline{P} = (1, -1)$$

$$6\underline{P} = (24, 116)$$

$$7\underline{P} = (-20/9, -388/27)$$

$$8\underline{P} = (84/25, -52/125), \dots$$

The structure of $E(\mathbb{Q})$ In 1922, Mordell showed that $E(\mathbb{Q})$ is a finitely generated abelian group; that is, that all rational solutions on E may be generated using the addition law from a finite number of basic solutions. If T is the subgroup of points of finite order on $E(\mathbb{Q})$ then

$$E(\mathbb{Q}) \cong T \times \mathbb{Z}^g$$

for some finite number g . There is a rich body of theory concerning the structure and computation of $E(\mathbb{Q})$ and many unsolved but important conjectures with far-reaching consequences. These do not concern us here but the interested reader might like to consult [3] for a stimulating account.

Returning to the example above, it can be shown that $E(\mathbb{Q}) \cong \mathbb{Z}$ (i.e. no points of finite order except $\underline{0}$, and $g=1$) and that it is generated by $\underline{P} = (0, 4)$.

We need to state some more facts about an elliptic curve over the finite field F_p . Firstly, the group $E(F_p)$ (which is obviously finite) is either a cyclic group or the product of two cyclic groups.

Secondly, let N_p denote the number of points in $E(F_p)$. Its value will depend on E , that is the values of A and B modulo p . Define a_p by

$$N_p = p+1 - a_p.$$

Since $p+1$ represents the "expected" number of solutions of

$$y^2 \equiv x^3 + Ax + B \pmod{p}$$

including the point at infinity, the value a_p measures the discrepancy of N_p from its expected value. It is known (the Riemann Hypothesis for Abelian Varieties of dimension 1) that

$$-2\sqrt{p} < a_p < 2\sqrt{p}.$$

Moreover, for each integer a in this range, the number of elliptic curves over F_p with $0 \leq A < p$, $0 \leq B < p$ and having $N_p = p+1 - a$ is

$$h(4p-a^2) * (p-1)/2$$

where $h(d)$ is the Hurwitz class number of discriminant $-d$. In particular, to every value a with $|a| < 2\sqrt{p}$, there is a corresponding elliptic curve E over F_p with $a_p = a$.

Example We consider the original example reduced modulo p with $p=5$:

$$E: y^2 = x^3 - x + 1.$$

To determine N_p consider the values of the cubic and thus y for each possible x :

x	0	1	2	3	4	∞
x^3-x+1	1	1	2	0	1	∞
y	± 1	± 1		0	± 1	∞

Thus $N_5 = 8$ and $a_5 = -2$. That $E(F_5)$ is cyclic of order 8 can be clearly seen by reducing $\underline{p}$, $2\underline{p}$, ..., $8\underline{p}$ from $E(Q)$ to $E(F_5)$ by considering each co-ordinate mod 5. In particular

$$8\underline{p} = (84/25, -52/125) + (\infty, \infty) = \underline{0}$$

2. b-smooth numbers

Let b be a positive integer. A number m is said to be b-smooth if every prime factor q of m is less than or equal to b . Thus

$$m = \prod_{q \leq b} q^{e_q} \quad \text{with} \quad e_q \geq 0.$$

Numbers which are b -smooth are rare. The probability that a random number $m \leq x$ is b -smooth is about u^{-u} where $u = \log x / \log b$. Thus, for example, if $x = 10^{100}$ and $b = 10^{10}$, then $u = 10$ and we see that the probability is 10^{-10} .

3. Pollard's p-1 method

The easiest way to understand Lenstra's factorisation method is to look first at Pollard's so-called $p-1$ method since certain strong

analogies can be drawn.

Suppose that the number n is to be factorised and that it is known that it has a prime divisor p for which $p-1$ is b -smooth. Define M by:

$$M = \prod_{q \leq b} q^{\lfloor \log n / \log q \rfloor}.$$

The exponents of q have been chosen so that we can guarantee that $p-1$ divides M . In particular, for any integer a with $(a, p) = 1$

$$a^{p-1} \equiv 1 \pmod{p}$$

and so

$$a^M \equiv 1 \pmod{p}.$$

To find p then, the method first computes $d \equiv a^M - 1 \pmod{n}$ for some random a - for example $a=2$; secondly it computes the highest common factor of d and n . This will normally be p unless there are other primes q dividing n for which the exponent of $a \pmod{q}$ divides M .

The time for this method is dominated by the time to compute a^M modulo n . Using the divide and conquer technique for evaluation of powers, this can be achieved in $O(\log M)$ modulo n multiplication steps. Hence since $\log M = \sum_{q \leq b} \log q$ the time is $O(b(\log n)^2 / \log b)$.

In view of the earlier remark about the rarity of b -smooth numbers, this method is not worth implementing unless it is known that, for some small b , $p-1$ is b -smooth.

4. Lenstra's method

The crucial results that made Pollard's $p-1$ method successful were that the residues modulo p formed a multiplicative group of order $p-1$, and so $a^{p-1} \equiv 1 \pmod{p}$, and that $p-1$ was b -smooth.

Lenstra's method is based on the same idea. But instead it uses the group (written additively) of points on an elliptic curve E over F_p which has order N_p . It too succeeds whenever N_p is b -smooth. The advantage of the elliptic curve method is that there are a large number of different curves E that can be tried, each with a potentially different value of N_p . For a large number of tries, the hope is that one such N_p is b -smooth for some suitably chosen small number b .

Explicitly, the method is as follows:

- Step 1 Choose a value for b (see later for optimal value) and let $M = b!$ or $M = \text{lcm}(1, 2, \dots, b)$ or some similar large b -smooth number.
- Step 2 Choose an elliptic curve E over $\mathbb{Q}$ at random and a point $\underline{P}$ that satisfies the equation modulo n .
- Step 3 Compute $M\underline{P}$ modulo n using the formulae given in section 1. If this computation fails to give a factor of n go back to Step 2 and choose a different curve E .

How does the computation of $M\underline{P}$ modulo n yield a factor of n ? The addition formulae supplied were for computation over a field. The formula for m , the gradient, involves one division; now over a field, this causes no problem because if the denominator is zero then the required sum is the point $\underline{Q} = (\infty, \infty)$. Modulo a composite number n , however, the division is only possible if the denominator d is co-prime to n . So the computation "fails" whenever $(d, n) > 1$. In particular, it fails when p is a divisor of n and N_p divides M . This failure however gives a factorisation of n and signifies, in fact, the success of the method.

The method then successfully factors n when the value of N_p for the chosen elliptic curve is a b -smooth number dividing M and there is a q dividing n such that the order of $\underline{P}$ in $E(\mathbb{F}_q)$ does not divide M .

Example The method is illustrated by attempting to factorise $n=187$ with $b=3$, $M=3!=6$ and $\underline{P}=(0,5)$ on the curve

$$E: y^2 = x^3 + x + 25.$$

To compute $\underline{P} + \underline{P}$: $M = 1/10 \equiv -56 \pmod{187}$ and $2\underline{P} = (-43, 18)$.

To compute $2\underline{P} + 2\underline{P}$: $M = (-62)/36 \equiv 71 \pmod{187}$ and $4\underline{P} = (78, -7)$.

To compute $2\underline{P} + 4\underline{P}$: $M = (-25)/(-66)$.

But $(-66, 187) = 11$; thus in three steps, the method produces the factor 11 of 187.

5. Concluding Remarks

The following theorem is due to Lenstra. The proof makes one "reasonable" assumption about the number of b -smooth numbers in a small interval.

Theorem The elliptic curve method with $b = L(p)^{1/\sqrt{2}}$ splits any integer n in expected time $O(L(p)^{\sqrt{2}+o(1)} (\log n)^2)$ where p is the smallest prime divisor of n .

Corollary The elliptic curve method can be used to factor completely any n in expected time $O(L(n)^{1+o(1)})$.

These results show that asymptotically, Lenstra's method is as good as any previously known method to factorise n . It has, however, in addition several important advantages. Firstly, it is easy to program, a non-sophisticated version requiring about 100 lines of code. Secondly, it requires very little storage and can be conveniently run as a background job. Thirdly, if n has a small prime factor, this can be expected to be found sooner than larger ones and helps to terminate the method in a shorter time. The previous fast methods operated in time which is independent of the size of the factors. Fourthly, it is ideally suited to implementation in parallel; many elliptic curves can be tried simultaneously and independently.

In practice, with the implementations so far, the method is not as fast as existing methods when applied to composite numbers which are the product of two large primes. To the author's knowledge the best results using Lenstra's method have been achieved by P. Montgomery [4] who has for example successfully factored the 74 digit number

$$(5^{106} + 1)/2$$

into two factors, one of which is approximately 10^{22} .

There are various implementation techniques to speed up the method of factorisation described in this article. Many of these techniques are improved by practical experimentation and it is the author's view that the method has not been around long enough to achieve its best potential. One of the crucial problems in increasing the speed of the method is to avoid too many inversions modulo n . Another is to make a sensible choice of b and of M . Clearly small primes in M need to have a higher exponent than big primes. Experiments indicate that whereas $M=b!$ has the exponents of small primes too big, $M=\text{lcm}(1, \dots, b)$ has the exponents too small.

6. References

1. H.W.Lenstra Jr. Elliptic Curve Factorisation and Primality Testing. Paper to Computational Number Theory Conference at Arcata, California. August 1985.
2. R. Silverman, Paper to Computational Number Theory Conference at Arcata, California. August 1985.
3. N.Koblitz. Introduction to Elliptic Curves and Modular Forms. Springer-Verlag 1984.
4. P.L.Montgomery. Experiences using Elliptic Curve Method of Factorisation. Paper to Computational Number Theory Conference at Arcata, California. August 1985.