RC 20223 (10/11/95, revised 11/08/95)
Computer Science / Mathematics

IBM Research Report

Finding a Small Root of a Univariate Modular Equation

Don Coppersmith

IBM Research Division
T.J. Watson Research Center
Yorktown Heights, New York

Finding a Small Root of a Univariate Modular Equation

Don Coppersmith*

Abstract

We show how to solve a polynomial equation (mod N) of degree k in a single variable x, as long as there is a solution less than about $N^{1/k}$. We give an application to an RSA encryption protocol: if messages are padded with truly random padding and then encrypted with an exponent 3, then two encryptions of the same message (with different padding) will reveal the message, as long as the padding is less than 1/9 of the length of N. With several encryptions, another technique can (heuristically) tolerate padding up to about 1/6 of the length of N.

1 Introduction

Let N be a large composite integer of unknown factorization. Let

$$p(x) = x^k + a_{k-1}x^{k-1} + ... + a_2x^2 + a_1x + a_0$$

be an integer polynomial of degree k in a single variable x, which we may assume to be monic. Suppose there is an integer solution y to

$$p(y) = 0 \pmod N$$

satisfying

$$|y| < \frac{1}{2}N^{(1/k)-\epsilon}.$$

We show how to find such a solution y, using lattice basis reduction techniques, in time polynomial in $(logN, k, \frac{1}{\epsilon})$.

An important application is to RSA encryption with small exponents and random padding. Suppose a message m is padded with a random value r before encryption with a small exponent such as $e = 3$, so that the ciphertext is

$$c = (m + r)^3 \pmod N.$$

Suppose it happens that a single message is encrypted twice, using different values of the random padding:

$$c_1 = (m + r_1)^3 \pmod N,$$

$$c_2 = (m + r_2)^3 \pmod N.$$

*IBM T.J. Watson Research Center, Yorktown Heights, New York, USA; copper@watson.ibm.com

From these two ciphertexts we can recover an equation of degree 9 in the quantity $r_2 - r_1$ (using the resultant), and if r_1 and r_2 are small – less than 1/9 of the length of N – then we can solve that equation for $r_2 - r_1$. Then, using techniques developed by Franklin and Reiter [1], we recover the original message $m + r_1$.

This can be viewed as a warning that, when using of RSA with small exponents, the use of random padding might not be helpful and might even be dangerous.

2 Solving a univariate polynomial

We show first how to find small solutions to $p(x) = 0 \pmod{N}$. Begin by selecting an integer $h > (k + \epsilon k - 1)/(\epsilon k^2) \approx 1/(k\epsilon)$ so that

$$h - 1 > (hk - 1)\left(\frac{1}{k} - \epsilon\right).$$

Evidently we must have $h, k \geq 2$.

For each pair of integers i, j satisfying $0 \leq i < k$, $1 \leq j < h$, we set

$$q_{i,j}(x) = x^i p(x)^j$$

and remark that, for the desired solution y, we know

$$q_{i,j}(y) = 0 \pmod{N^j}.$$

Indeed, setting

$$z = \frac{p(y)}{N}$$

and noting that z is an integer, we see that

$$q_{i,j}(y) = y^i z^j N^j.$$

We build a rational matrix M of size $(2hk-k)\times(2hk-k)$, using the coefficients of the polynomials $q_{i,j}(x)$, in such a way that an integer linear combination of the rows of M corresponding to powers of y will give a vector with relatively small Euclidean norm. Further, all such short vectors will satisfy a certain linear relation which we will discover by lattice basis reduction techniques [2]; this relation will translate to a polynomial relation on y over $\mathbf{Z}$ (not mod N), which we can solve over $\mathbf{Z}$ to discover y.

The matrix M is broken into blocks. The upper right block, of size $(hk) \times (hk - k)$, has rows indexed by the integer g with $0 \leq g < hk$, and columns indexed by $\gamma(i, j) = hk + i + j(k - 1)$ with $0 \leq i < k$ and $1 \leq j < h$, so that $hk \leq \gamma(i, j) < 2hk - k$. The entry at $g, \gamma(i, j)$ is the coefficient of x^g in the polynomial $q_{i,j}(x)$.

The lower right $(hk - k) \times (hk - k)$ block is a diagonal matrix, with the value N^j in each column $\gamma(i, j)$.

The upper left $(hk) \times (hk)$ block is a diagonal matrix, whose value in row g is a rational approximation to $Y^{-g}/\sqrt{hk}$, where $Y = \frac{1}{2}N^{(1/k)-\epsilon}$ is an upper bound to $|y|$.

The lower left $(hk - k) \times (hk)$ block is zero.

We illustrate the matrix M in the case $h=3$, $k=2$. Assume that $p(x)=x^2+ax+b$ and $p(x)^2=x^4+cx^3+dx^2+ex+f$. For simplicity we write δ instead of $1/\sqrt{hk}$.

$$M=\begin{bmatrix}
\delta & 0 & 0 & 0 & 0 & 0 & b & 0 & f & 0\\
0 & \delta Y^{-1} & 0 & 0 & 0 & 0 & a & b & e & f\\
0 & 0 & \delta Y^{-2} & 0 & 0 & 0 & 1 & a & d & e\\
0 & 0 & 0 & \delta Y^{-3} & 0 & 0 & 0 & 1 & c & d\\
0 & 0 & 0 & 0 & \delta Y^{-4} & 0 & 0 & 0 & 1 & c\\
0 & 0 & 0 & 0 & 0 & \delta Y^{-5} & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & N & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & N & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & N^2 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & N^2
\end{bmatrix}$$

M is upper triangular. Its determinant is

$$det(M)=N^{kh(h-1)/2}Y^{-(hk)(hk-1)/2}/\sqrt{hk}^{hk}=(N^{h-1}Y^{-(hk-1)}(hk)^{-1})^{hk/2}.$$

Because $h,k\geq 2$, we know that $hk\leq 2^{hk-2}$. This implies

$$det(M)\geq (N^{h-1}Y^{-(hk-1)}2^{-(hk-2)})^{hk/2}.$$

Then from our choice of Y and h, we calculate

$$det(M)\geq (N^{h-1}(2Y)^{hk-1}2)^{hk/2}\geq (N^{(h-1)-(hk-1)((1/k)-\epsilon)}2)^{hk/2}\geq 2^{hk/2}>1.$$

We will do lattice basis reduction on the rows of M to find an expression for those integer linear combinations of rows of M with small Euclidean norm ("short" vectors).

One such short vector is related to the unknown solution y. Start with a row vector $\mathbf{r}$ whose left-hand elements are powers of y:

$$\mathbf{r}_g=y^g$$

and whose right-hand elements are the negatives of powers of y and z:

$$\mathbf{r}_{\gamma(i,j)}=-y^iz^j$$

$$\mathbf{r}=(1,y,y^2,...,y^{hk-1},-z,-yz,...,-y^{k-1}z,-z^2,-yz^2,...,-y^{k-1}z^{h-1}).$$

The product $\mathrm{s}=\mathbf{r}M$ is a row vector with left-hand elements given by

$$\mathrm{s}_g=(y/Y)^g/\sqrt{hk}$$

and right-hand elements by

$$\mathrm{s}_{\gamma(i,j)}=q_{i,j}(y)-y^iz^jN^j=0.$$

The Euclidean norm of s is estimated by:

$$||\mathrm{s}||=\left[\sum_g \mathrm{s}_g{}^2\right]^{1/2}\leq\left[\sum_g(1/\sqrt{hk})^2\right]^{1/2}=1.$$

Because $det(M) > 1$, when we apply lattice basis reduction to the rows of M we will find a reduced basis, some of whose elements must be longer than 1. Since $||\mathbf{s}|| \leq 1$, $\mathbf{s}$ is an integer linear combination of basis elements which are all shorter than 1. This restricts $\mathbf{s}$ to a sublattice of M, and will give us the equation on y which we need.

Because $p(x)$ and hence $q_{i,j}(x)$ are monic polynomials, the lower $hk-k$ rows of the upper right block of M form an upper triangular matrix with 1 on the diagonal. This implies that we can do elementary row operations on M to produce a block matrix $\tilde{M}$ whose lower right $(hk-k)\times(hk-k)$ block is the identity and whose upper right $(hk)\times(hk-k)$ block is zero. The upper left $(hk)\times(hk)$ block $\hat{M}$ satisfies $det(\hat{M}) = det(M) > 1$.

We now restrict our attention to the upper hk rows of $\tilde{M}$, or equivalently on $\hat{M}$: the lattice elements represented by vectors whose right-hand side is 0.

We do lattice basis reduction on $\hat{M}$, and continue to call the result $\hat{M}$. The determinant does not change. Any reduced basis of $\hat{M}$ will have at least one row with Euclidean norm exceeding $2^{1/4}$:

$$\Pi_g(||row_g(\hat{M})||) \geq det(\hat{M}) \geq 2^{hk/2} > (2^{1/4})^{2hk-k}.$$

We may assume the largest row to be $||row_0(\hat{M})|| > 2^{1/4}$. Because the basis is reduced, any integer combination of rows which includes row_0 nontrivially will also have length exceeding $2^{1/4}$. This implies that any lattice element of length at most 1 is an integer combination of rows 1 through $hk-1$ of $\hat{M}$.

(*Remark:* We can accommodate some inexactness in the lattice reduction algorithm. For each $L = 0, 1, ..., hk-1$, the first L elements of the computed reduced basis define a subspace of $\mathbf{R}^{hk}$. Project to that subspace and take determinants to find a fundamental volume. Suppose (by induction) that this volume is less than $2^{L/4}$. Project the remaining basis elements to the orthogonal complementary subspace of $\mathbf{R}^{hk}$. In the resulting lattice of dimension $hk-L$ we need to either find a vector of length less than $2^{1/4}$ or show that no vectors exist of length less than 1. In the former case, adjoin the vector to the first L and continue by induction; the volume has increased by a factor less than $2^{1/4}$. In the latter case, we have shown that all short vectors (length less than 1) lie in the space of dimension L.)

In terms of the original matrix M, let a short lattice element (with 0 in the right-hand side) be given by

$$(b_0, b_1, ..., b_{hk-1}, d_{\gamma(0,1)}, ..., d_{\gamma(k-1,h-1)})M.$$

Because these short rows span a vector space of dimension at most $hk-1$, simple linear algebra can produce a collection of integers $c_0, c_1, ..., c_{hk-1}$ (not all zero) satisfying

$$\sum_g c_g b_g = 0$$

for each short row; this equation holds over $\mathbf{Z}$. (Notice that the $d_{\gamma(i,j)}$ are not involved.)

Our unknown solution row $\mathbf{s} = \mathbf{r}M$ is such a short row, with $b_g = \mathbf{r}_g = y^g$. So it must be true that

$$\sum_g c_g b_g = \sum_g c_g y^g = 0.$$

Notice that this equation holds in $\mathbf{Z}$, not just mod N. We can solve this for y in polynomial time, using known techniques for solving univariate polynomial equations over $\mathbf{Z}$. Thus we have produce the desired solution y.

Remark: If there are several short solutions y, this procedure will find all of them simultaneously.

3 Extension to Multivariate Polynomials

We encountered some technical difficulties trying to extend this procedure to multivariate polynomials. The guarantee breaks down at a crucial step, so this extension is heuristic. Our sketch is brief because this is irrelevant to the present application.

If we are given a polynomial $p(x_1, ..., x_m) \pmod N$ of total degree k, and we know there is a solution $x_i = y_i$ with $|y_i| < N^{\alpha_i}$, we hope to find this solution as long as $\sum \alpha_i < (1/k) - \epsilon$.

Define $z = p(y_1, ..., y_m)/N$. Define $q_{i_1 ... i_m j}(x_1, ..., x_m) = x_1^{i_1} x_2^{i_2} ... x_m^{i_m} p(x_1 ... x_m)^j$ and notice that $q_{i_1 ... i_m j}(y_1, ..., y_m)$ is divisible by N^j. Set a limit T and develop the modular equations $q_{i_1 ... i_m j}(y_1, ..., y_m) = 0 \pmod{N^j}$ for all nonnegative integer indices $(i_1, ..., i_m, j)$ with $i_m < k$ and $i_1 + i_2 + ... + i_m + kj \leq T$.

Build the matrix M analogous to that of Section 2. The vector $\mathbf{r}$ contains all monomials of total degree at most T, so the sum of the total degrees of these monomials is $m \begin{pmatrix} T+m \\ m+1 \end{pmatrix}$, and the sum of the degrees in each $x_i, i = 1, 2, ..., m-1$, is $\begin{pmatrix} T+m \\ m+1 \end{pmatrix}$. These appear as negative exponents of α_i in the diagonal entries of the upper left block of M.

The powers of N appearing in the lower right of M (the moduli) add to

$$\frac{1}{k} \begin{pmatrix} T+m \\ m+1 \end{pmatrix} - O(\begin{pmatrix} T+m \\ m \end{pmatrix})$$

(asymptotically for large T). With the requirement $\sum \alpha_i < (1/k) - \epsilon$, we will have $det(M) > 1$.

The vector s will be shorter than 1, so will be among the shorter vectors in the lattice. By the methods of Section 2 we can get at least one polynomial equation satisfied by the y_i over $\mathbf{Z}$. But to solve for y_i over $\mathbf{Z}$ we would need m independent equations. We might or might not get the required equations, so the procedure might work or might fail in a particular application. Much work needs to be done in this area.

4 Application to RSA with Random Padding

The present work was motivated by the following result of Franklin and Reiter [1]. Suppose two messages m and m' satisfy a *known* affine relation, say

$$m' = m + r$$

with r known. Suppose we know the RSA-encryptions of the two messages with an exponent of 3:

$$\begin{aligned} c &= m^3 && \pmod N \\ c' &= (m')^3 = m^3 + 3m^2 r + 3mr^2 + r^3 && \pmod N \end{aligned}$$

Then we can recover m from c, c', r and N:

$$m = \frac{r(c' + 2c - r^3)}{c' - c + 2r^3} = \frac{r(3m^3 + 3m^2 r + 3mr^2)}{3m^2 r + 3mr^2 + 3r^3} \pmod N$$

What if we do not know the exact relation between m and m', but we do know that r is small, say

$$\begin{aligned} m' &= m + r \\ |r| &< N^{(1/9)-\epsilon} \end{aligned}$$

Can we still find m?

One can imagine a protocol in which messages M are subjected to random padding before being RSA-encrypted with an exponent of 3. Perhaps M is left-shifted by k bits, and a random k-bit quantity R is added, to form a plaintext m; the ciphertext c is then the cube of $m \pmod N$:

$$c = m^3 = (2^k M + R)^3 \pmod N$$

Now suppose the same message is encrypted twice, but with a different random pad each time. Let the second random pad be $R' = R + r$ so that the second plaintext is $m' = m + r$. Then we see the two ciphertexts

$$\begin{aligned} c &= m^3 &&= (2^k M + R)^3 && \pmod N \\ c' &= (m')^3 &&= (2^k M + R')^3 = (m+r)^3 && \pmod N \end{aligned}$$

Can we recover r and m?

We can eliminate m from the two equations above by taking their resultant:

$$\begin{aligned} \mathit{Resultant}_m \quad & (m^3 - c, (m+r)^3 - c') = \\ & = r^9 + (3c - 3c')r^6 + (3c^2 + 21cc' + 3(c')^2)r^3 + (c - c')^3 = 0 \pmod N \end{aligned}$$

This is a univariate polynomial in r of degree 9 (mod N). If $|r| < N^{(1/9)-\epsilon}$, we can apply the present work to recover r. We can then apply Franklin and Reiter's result to recover m, and strip off the padding to get M.

This works just as well if the padding goes in the high order bits, or in the middle; just divide each plaintext by the appropriate power of 2 to move the random bits to the low order bits.

The warning is clear: If the message is subject to random padding of length less than 1/9 the length of N, and then encrypted with an exponent of 3, multiple encryptions of the same message will reveal the message.

Notice that for a 1024-bit RSA key, this attack tolerates 100 bits of padding fairly easily.

Some possible steps to avoid this attack:

(1) Spread the random padding into several blocks (not one contiguous block). Then the present attack needs to be modified, and apparently will tolerate only a smaller total amount of padding. The padding could be two small blocks r and s, positioned so that the encryption is $c = (2^l r + 2^k m + s)^3 \pmod N$. Two encryptions of the same message would yield a resultant which is a single equation in two small integer variables r and s. The generalized attack of Section 3 might work, provided that $|r|$ and $|s|$ are subject to bounds R and S with $RS < N^{(1/9)-\epsilon}$. The computation is more complicated and results are not guaranteed.

(2) Spread the padding throughout the message: four bits out of each eight-bit byte, for example. This seems to be a more effective defense against the present attack.

(3) Increase the amount of padding. This decreases efficiency; also if the padding is less than 1/6 the length of N, the alternate solution shown in Section 5 might still recover the message if multiple encryptions have been done.

(4) Make the "random" padding depend on the message deterministically. For example we could subject the message to a hashing function, and append that hash value as the random padding. Then two encryptions would be identical, because the random padding would be identical. A possible weakness still exists: suppose a time-stamp is included in each message, and this time-stamp occupies the low order bits, next to the padding. Then two plaintexts for the same message (with different time stamps) will differ in the time-stamp and (possibly) the pad; just let r combine these two fields and proceed as before.

(5) Use larger exponents for RSA encryption. If the exponent is e, the attack apparently tolerates random padding of length up to $1/e^2$ times the length of N. So already for $e = 7$ the attack is useless: on a 1024-bit RSA key with $e = 7$, the attack would tolerate only 21 bits of padding, and this would be better treated by exhaustion.

5 Another Solution for Multiple Encryptions

If instead of two encryptions of the same message we have several, say $k + 1$, then we can mount other attacks which might tolerate larger fields of random padding. We sketch here an attack which (heuristically) seems to tolerate random padding up to α times the length of N where

$$\alpha < \frac{k-2}{6k-3} < \frac{1}{6}.$$

We begin with

$$\begin{aligned} A_0 &= m^3 && \pmod N \\ A_i &= (m + r_i)^3 && \pmod N \\ c_i = A_i - A_0 &= 3m^2 r_i + 3m r_i^2 + r_i^3 && \pmod N \end{aligned}$$

where we know A_0, A_i, c_i and N, but not m or r_i. We assume the padding is small:

$$|r_i| \leq \frac{1}{2} N^\alpha.$$

For indices $i < j < p$ define $d_{ij} = r_i r_j (r_i - r_j)$ and $e_{ijp} = -r_i r_j r_p (r_i - r_j)(r_j - r_p)(r_p - r_i)$. The $C(k,2) = \begin{pmatrix} k \\ 2 \end{pmatrix}$ linearly independent quantities d_{ij} each satisfy $|d_{ij}| < N^{3\alpha}$, and the $C(k,3)$ linearly independent quantities e_{ijp} each satisfy $|e_{ijp}| < N^{6\alpha}$. One can check the following identity:

$$d_{ij} c_p + d_{jp} c_i - d_{ip} c_j = e_{ijp} \pmod N.$$

This suggests lattice basis reduction on the row basis of the following matrix. M is a square upper triangular integer matrix of dimension $(C(k,2) + C(k,3))$. Its upper left $C(k,2) \times C(k,2)$ block is the identity times an integer approximation to $N^{3\alpha}$. Its lower left $C(k,3) \times C(k,2)$ block is 0. Its lower right $C(k,3) \times C(k,3)$ block is N times the identity. Its upper right $C(k,2) \times C(k,3)$ block has rows indexed by pairs of indices $(i,j), i < j$, and columns indexed by triples of indices $(i,j,p), i < j < p$. Column (i,j,p) has three nonzero entries: c_p at row (i,j), c_i at row (j,p), and $-c_j$ at row (i,p).

We illustrate the matrix M for the case $k=4$. The first $C(k,2)=6$ rows are indexed by (1,2), (1,3), (1,4), (2,3), (2,4) and (3,4). The last $C(k,3)=4$ columns are indexed by (1,2,3), (1,2,4), (1,3,4) and (2,3,4).

$$M = \begin{bmatrix} N^{3\alpha} & 0 & 0 & 0 & 0 & 0 & c_3 & c_4 & 0 & 0 \\ 0 & N^{3\alpha} & 0 & 0 & 0 & 0 & -c_2 & 0 & c_4 & 0 \\ 0 & 0 & N^{3\alpha} & 0 & 0 & 0 & 0 & -c_2 & -c_3 & 0 \\ 0 & 0 & 0 & N^{3\alpha} & 0 & 0 & c_1 & 0 & 0 & c_4 \\ 0 & 0 & 0 & 0 & N^{3\alpha} & 0 & 0 & c_1 & 0 & -c_3 \\ 0 & 0 & 0 & 0 & 0 & N^{3\alpha} & 0 & 0 & c_1 & c_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & N & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & N & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & N & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & N \end{bmatrix}$$

Consider the integer row vector $\mathbf{r}$ whose first $C(k,2)$ entries are d_{ij}, and whose last $C(k,3)$ entries are the integers $(e_{ijp} - (d_{ij}c_p + d_{jp}c_i - d_{ip}c_j))/N$. The product $\mathbf{r}M = \mathrm{s}$ has left-hand elements $d_{ij}N^{3\alpha}$ and right-hand elements e_{ijp}; all its entries are bounded by $N^{6\alpha}$. We hope that lattice basis reduction will find this row.

The determinant of M is $N^{3\alpha C(k,2)+C(k,3)}$. choice of α, This is larger than $(N^{6\alpha})^{C(k,2)+C(k,3)}$ because of our choice of α. So s is among the shorter elements of the lattice generated by the rows of M.

The difficulty in finding s depends on its rank among the short elements. If $|r_i|$ are much smaller than N^α then we can hope that s is the shortest lattice element, and that lattice basis reduction methods can recover it efficiently. We do not here supply efficiency estimates or probabilities of success; we treat this as a heuristic attack.

Assuming that we can actually find s, we will be able to recover the values r_i by taking *g.c.d.* of elements of $\mathbf{r} = \mathrm{s}M^{-1}$:

$$g.c.d.\{d_{1,2}, d_{1,3}, ..., d_{1,k}\} = g.c.d.\{r_1r_2(r_1-r_2), r_1r_3(r_1-r_3), ..., r_1r_k(r_1-r_k)\}$$

$$= r_1 \times g.c.d.\{r_2(r_1-r_2), r_3(r_1-r_3), ..., r_k(r_1-r_k)\},$$

and hopefully the latter *g.c.d.* will be small enough to discover by exhaustive search. Having found r_i, we can recover m by Franklin and Reiter's technique.

If we have 14 encryptions of the same message ($k=13$), then we can tolerate a random padding of about 150 bits in a 1024-bit RSA message.

6 RSA with Stereotyped Messages

An easy application is to RSA encryption with low exponent where most of the message is fixed or "stereotyped".

Suppose the plaintext consists of two pieces:

(1) A known piece $B = 2^k b$, such as the ASCII representation of "October 19, 1995. The secret key for the day is"

(2) An unknown piece m, such as "Squeamish Ossifrage".

If we know B and $c = (B+m)^3 \pmod N$, then we can recover m as long as $|m| < N^{(1/3)-\epsilon}$. This is obvious when $B = 0$, but the present paper makes it possible for nonzero B as well.

7 Conclusions and Open Problems

We have shown how to solve a univariate polynomial equation (mod N) of degree k if there is a solution smaller than $N^{(1/k)-\epsilon}$. We have applied this to the case of RSA encryption with exponent 3 with random padding of less than 1/9 (resp. 1/6) of the length of N, to recover a message which has been enciphered twice (resp. several times) with different random padding each time.

We warn against RSA encryption with exponent 3 and with random padding of such length, in the case where a protocol allows a message to be enciphered several times with different values of the padding.

An important open problem is to find conditions under which the multivariate case works. In particular, how effectively does it work for the case of two messages with random padding in two blocks?

8 Acknowledgements

The author gratefully acknowledges enlightening discussions with Andrew Odlyzko. Matt Franklin and Mike Reiter's Crypto 95 rump session paper and subsequent discussions were useful. Jacques Patarin was independently working on the idea of unknown offsets in the RSA setting.

References

[1] M. Franklin and M. Reiter, "A Linear Protocol Failure for RSA with Exponent Three," rump session, Crypto 95 (not in proceedings).

[2] A.K. Lenstra, H.W. Lenstra and L. Lovasz, "Factoring Polynomials with Integer Coefficients," *Matematische Annalen* vol. 261 (1982), 513-534.