Solving low degree polynomials

Asiacrypt 2003, Taipei, December 1, 2003

Don Coppersmith
IBM T.J. Watson Research Center
Yorktown Heights, New York, USA
www.research.ibm.com/people/c/copper

Outline

- History
- Motivation
- Results
- Potential improvements
- Applications

Results (preview)

Given an integer N, and a polynomial $p(x)$ in one variable, defined $\bmod N$, of degree d, and the bound $B = N^{1/d}$, we can efficiently find all solutions x_0 satisfying

$$|x_0| < B$$
$$p(x_0) = 0 \bmod N$$

References

- Eurocrypt 1996 (**LNCS 1070**)
  - DC, Matthew Franklin, Jacques Patarin, Michael Reiter, "Low-exponent RSA with related messages"
  - DC, "Finding a small root of a univariate modular equation"
  - DC, "Finding a small root of a bivariate integer equation; factoring with high bits known,"

- *J. Cryptology* **Vol 10**, No. 4, Autumn 1997
  - DC, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities"

- CaLC 2001 (Cryptography and Lattices Conference, **LNCS 2146**)
  - DC, “Finding Small Solutions to Small Degree Polynomials”

Two related messages (Matt Franklin, Michael Reiter)

RSA encryption: $e = 3$

$$N = pq$$
$$c = m^3 \pmod N$$
$$b = (m+1)^3 \pmod N$$

$$(b+2c-1)/(b-c+2) = [(m^3+3m^2+3m+1)+2m^3-1]/[(m^3+3m^2+3m+1)-m^3+2]$$

$$= [3m^3 + 3m^2 + 3m]/[3m^2 + 3m + 3]$$
$$= m \pmod N$$

Generalize?

$$\begin{aligned} e &= 5 \\ c &= m^5 \pmod{N} \\ b &= (m+1)^5 \pmod{N} \end{aligned}$$

$$m = \frac{2b^3 - b^2c - 4bc^2 + 3c^3 + 14b^2 - 88bc - 51c^2 - 9b + 64c - 7}{b^3 - 3b^2c + 3bc^2 - c^3 + 37b^2 + 176bc + 37c^2 + 73b - 73c + 14}$$

- You can continue for other values of e.
- It gets harder.

Polynomials in m, treating b, c as given constants, evaluating to $0 \pmod N$ at m_0:

$$\begin{aligned} m^5 - c &= 0 \bmod N \\ (m+1)^5 - c &= 0 \bmod N \\ \gcd(m^5 - c, (m+1)^5 - b) &= m - m_0 \in \mathbb{Z}/N[m] \text{ usually} \end{aligned}$$

E.g. $\gcd(m^5 - 43, (m+1)^5 - 4) = m - 5 \in \mathbb{Z}/67[m]$

But not always:

$$\begin{aligned} \gcd(m^{31} - 29, (m+1)^{31} - 30) &= m^4 + 36m^3 + 53m^2 + 10m + 29 \\ &= (m - 29)(m^3 - 2m^2 - 5m - 1) \\ &\in \mathbb{Z}/67[m] \end{aligned}$$

Known difference

Just as easy if known difference between messages:

$$\begin{array}{rcl} c & = & m^3 \bmod N \\ b & = & (m+y)^3 \bmod N \\ \text{Known:} & & c, b, y, N \\ \text{Unknown:} & & m \end{array}$$

$$\gcd(m^3 - c, (m+y)^3 - b) = m - m_0 \in \mathbb{Z}/N[m]$$

Small unknown difference

What if the difference is small but unknown?

$$\begin{array}{rcl} c & = & m^3 \bmod N \\ b & = & (m+y)^3 \bmod N \\ \text{Known:} & & c, b, N \\ \text{Unknown:} & & m, y, \quad \text{with} \quad y \quad \text{small} \end{array}$$

Example:

$m =$ “0.14 micron technology to be announced 2 December 2003.
$4.85 IBM stock jump anticipated. gr3172680994”

$m + y =$ “0.14 micron technology to be announced 2 December 2003.
$4.85 IBM stock jump anticipated. jb5637124412”

“gr3172680994”, “jb5637124412” random padding for security.

y= “jb5637124412” - “gr3172680994” is small.

Resultant:

$$Res_m(m^3 - c, (m + y)^3 - b) \in \mathbb{Z}/N[y]$$

The resultant is a polynomial in y which results from eliminating m from the first two equations; if (m, y) simultaneously satisfies the first two equations, then y satisfies the resultant.

Resultant example

$$\begin{aligned} N &= 67 \\ e &= 2 \\ c &= m^2 & = 39 \bmod N \\ b &= (m+y)^2 & = -7 \bmod N \end{aligned}$$

$$R(y) = Res_m(m^2 - 39, (m+y)^2 + 7) \in \mathbb{Z}/67[y]$$

$$P(m,y) \times (m^2 - 39) + Q(m,y) \times ((m+y)^2 + 7) = R(y)$$

$$(2my+3y^2+21)\times(m^2-39)+(-2my+y^2-21)((m+y)^2+7) = y^4+3y^2-28$$

$$Res_m(m^2-39,(m+y)^2+7)=\det\begin{bmatrix}1 & 0 & -39 & 0\\ 0 & 1 & 0 & -39\\ 1 & 2y & y^2+7 & 0\\ 0 & 1 & 2y & y^2+7\end{bmatrix}$$

Two (=deg($(m+y)^2+7$)) rows of coefficients of m^2-39 (as polynomial in m), staggered:

$$[1,0,-39]\Leftrightarrow 1m^2+0m^1+(-39)m^0;$$

then two rows of coefficients of $(m+y)^2+7$, staggered:

$$[1,2y,y^2+7]\Leftrightarrow 1m^2+(2y)m^1+(y^2+7)m^0.$$

$Res_m(m^2 - 39, (m+y)^2 + 7) = y^4 + 3y^2 - 28$ (over $\mathbb{Z}/67$)
is a polynomial of degree 4 in y $(4 = 2 \times 2)$.

$Res_m(m^3 - 16, (m+y)^3 - 43)$ (over $\mathbb{Z}/67$) is a polynomial of degree 9 in y $(9 = 3 \times 3)$:

$$Res_m(m^3 - 16, (m+y)^3 - 43) = y^9 + 50y^6 + 2y^3 + 24 \in \mathbb{Z}/67[y]$$

with some small solution y.

Could we solve such an equation?

Second example (more natural)

Message = "The password for today is Sashimi"

m_0="The password for today is — —" (known)
y="Sashimi" (unknown)
$c = (m_0 + y)^3 \bmod N$
Known: c, m_0, N. Unknown but small: y.

$$p(y) = (m_0 + y)^3 - c = 0 \bmod N$$

"Small" unknown y; polynomial P has "low" degree 3.

Unifying theme

- Polynomial $p(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_1 x + p_0$
- Modulus N (large integer, unknown factorization)
- "Low" degree d
- "Small" solution x_0:
- Bound B, existence of $x_0 \in \mathbb{Z}$ with $|x_0| < B$ and $p(x_0) = 0 \bmod N$.

Goal:

- Tolerate B as large as possible, as a function of N and d.

- Find all x_0 satisfying bound and polynomial.

First try — Johan Håstad

Collection C_1 of $d+1$ polynomials:

$$C_1 = \{x^i, 0 \leqslant i < d\} \cup \{p(x)/N\}$$

For each polynomial $q \in C_1$, each small root x_0: $q(x_0)$ is an integer.
Same is true of any integer combination of polynomials in C_1.

Lattice generated by $d+1$ columns of real matrix:

$$L_1 = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & p_0/N \\ 0 & B & 0 & \cdots & 0 & 0 & p_1 B/N \\ 0 & 0 & B^2 & \cdots & 0 & 0 & p_2 B^2/N \\ & & & \vdots & & & \\ 0 & 0 & 0 & \cdots & B^{d-2} & 0 & p_{d-2} B^{d-2}/N \\ 0 & 0 & 0 & \cdots & 0 & B^{d-1} & p_{d-1} B^{d-1}/N \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 B^d/N \end{bmatrix}$$

$$\left[1, \frac{x}{B}, \frac{x^2}{B^2}, \ldots, \frac{x^d}{B^d}\right] \times \begin{bmatrix} 0 & p_0/N \\ 0 & p_1 B/N \\ B^2 & p_2 B^2/N \\ 0 & p_3 B^3/N \\ \vdots & \vdots \\ 0 & p_{d-1} B^{d-1}/N \\ 0 & p_d B^d/N \end{bmatrix} = [x^2, p(x)/N]$$

Each column v is a polynomial $q(x) \in C_1$, expressed in basis x^i/B^i.
The ith element is coefficient of x^i in $q(x)$, times scaling factor B^i.

Lattice basis reduction (LLL).

$$\begin{aligned} \det(L_1) &= 1 \times B \times B^2 \times \cdots \times B^{d-1} \times (B^d/N) \\ &= B^{d(d+1)/2}/N \approx 1 \end{aligned}$$

(up to a constant depending on dimension d but not on N, B).
Lattice basis reduction gives a column v with bounded norm:

$$\sqrt{\sum v_i^2} \leqslant \gamma_d \times (\det(L_1))^{1/(d+1)} \approx 1$$

(Again γ_d depends only on d, not N or B).
$q(x_0)$ is an integer, but

$$\begin{array}{rcl} |q(x_0)| & \leqslant & \sum |q_i x_0^i| \\ & = & \sum |v_i (x_0/B)^i| \\ & \leqslant & \sum |v_i 1^i| \\ & \leqslant & (\sqrt{d+1} \times \gamma_d) B^{d/2} / N^{1/(d+1)} \\ & < & 1 \end{array}$$

We arrange that

$$det(L_1) \approx 1$$

$$B \approx N^{2/(d^2+d)}$$

Then $q(x_0) \in \mathbb{Z}$ and $|q(x_0)| < 1$ implies $q(x_0) = 0 \in \mathbb{R}$. (Not just $\mathbb{Z}/N$.)

Can solve $q(x_0) = 0 \in \mathbb{R}$ by ordinary methods.

Note: this gives all small solutions x_0.

.

Problem: $B = \gamma' N^{2/(d^2+d)}$ is small. Let's try to increase it.

Second try, improved B

Larger collection of $2d$ polynomials:

$$C_2 = \{x^i, 0 \leqslant i < d\} \cup \{(p(x)/N)x^i, 0 \leqslant i < d\}$$

$$L_2 = \begin{bmatrix} 1 & 0 & \cdots & 0 & p_0/N & 0 & \cdots & 0 \\ 0 & B & \cdots & 0 & p_1 B/N & p_0 B/N & \cdots & 0 \\ 0 & 0 & \cdots & 0 & p_2 B^2/N & p_1 B^2/N & \cdots & 0 \\ & & \vdots & & & & \vdots & \\ 0 & 0 & \cdots & 0 & p_{d-2} B^{d-2}/N & p_{d-3} B^{d-2}/N & \cdots & 0 \\ 0 & 0 & \cdots & B^{d-1} & p_{d-1} B^{d-1}/N & p_{d-2} B^{d-1}/N & \cdots & p_0 B^{d-1}/N \\ 0 & 0 & \cdots & 0 & 1B^d/N & p_{d-1} B^d/N & \cdots & p_1 B^d/N \\ 0 & 0 & \cdots & 0 & 0 & 1B^{d+1}/N & \cdots & p_2 B^{d+1}/N \\ & & \vdots & & & & \vdots & \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1B^{2d-1}/N \end{bmatrix}$$

Dimension$=2d$.
Determinant$=B^{0+1+\cdots+(2d-1)}/N^d = B^{d(2d-1)}/N^d$
As before, if we set $\det \approx 1$

$$(B \approx N^{1/(2d-1)})$$

then we get column vector norm < 1.
Improved bound from $B \approx N^{2/(d^2+d)}$ to $B \approx N^{1/(2d-1)}$.

Calculating the bounds

Need $\det L \approx 1$.
L is a triangular matrix; determinant is product of diagonal entries.

Calculating the bounds ...

First case, diagonal is

$$1, B, B^2, \ldots, B^{d-1}, B^d/N$$
$$\det L_1 = B^{0+1+2+\cdots+(d-1)+d}/N = B^{(d^2+d)/2}/N \approx 1$$
$$B \approx N^{2/(d^2+d)}$$

Second case, diagonal is

$$1, B, B^2, \ldots, B^{d-1}, B^d/N, B^{d+1}/N, \ldots, B^{2d-1}/N$$
$$\det L_2 = B^{0+1+2+\cdots+(2d-1)}/N^d = B^{2d^2-d}/N^d \approx 1$$
$$B \approx N^{1/(2d-1)}$$

Tightening the bounds

If $N|p(x_0)$, then $N^k|p(x_0)^k$.
Pick a parameter h: larger h gives larger matrix, more work, and better bounds B.

Larger collection of $d \times h$ polynomials:

$$C_3 = \{(p(x)/N)^k x^i, 0 \leqslant i < d, 0 \leqslant k < h\}$$

$$\dim(L_3) = dh$$

Diagonal entries of L_3 are

$$\{B^{i+dk}/N^k | 0 \leqslant i < d, 0 \leqslant k < h\}$$

$$\det(L_3) = \prod_{i,k} (B^{i+dk}/N^k) = B^{dh(dh-1)/2} N^{-dh(h-1)/2}$$

For $\det(L_3) \approx 1$ we need

$$B \approx N^{(h-1)/(dh-1)}$$

Fixing ϵ and picking h large ($h \approx 1/(d\epsilon)$), this becomes

$$B < O_{d,\epsilon}(N^{1/d-\epsilon})$$

So the natural bound appears to be

$$B \approx N^{1/d}$$

Results

Given an integer N, and a polynomial $p(x)$ in one variable, defined $\bmod N$, of degree d, and the bound $B = N^{1/d}$, we can efficiently find all solutions x_0 satisfying

$$|x_0| < B$$
$$p(x_0) = 0 \bmod N$$

"Efficient": time polynomial in $(d, \log N)$.

Summary of technique (one variable mod N)

Given $p(x)$ (degree d), N, $B \approx N^{1/d}$,

To find: x_0 such that $p(x_0) = 0 \bmod N$ and $|x_0| < B$

- Find real polynomials $q_i(x)$ with $q_i(x_0) \in \mathbb{Z}$ (at any root x_0)
- Lattice basis reduction: find $q(x)$, an integer combination of $q_i(x)$ with small coefficients
- $q(x_0) \in \mathbb{Z}$
- $|q(x_0)| < 1$ (when $|x_0| < B$)

- Therefore $q(x_0) = 0 \in \mathbb{R}$ (for all small roots)
- Solve $q(x_0) = 0 \in \mathbb{R}$ — easy
- This gives all valid x_0

Related — two variables

Given a polynomial $p(x)$ in two variables, defined over $\mathbb{Z}$ (not $\bmod N$ any more), we can define bound B_x, B_y in terms of the degree and coefficients of p. We can efficiently find all integer solutions (x_0, y_0) satisfying

$$|x_0| < B_x$$
$$|y_0| < B_y$$
$$p(x_0, y_0) = 0(\text{ in } \mathbb{Z})$$

Example:

$$p(x, y) = (P_0 + x) * (Q_0 + y) - N$$

where $P, Q \approx \sqrt{N}$.
Then $B_x = B_y = N^{1/4}$.
Factor N if we know half the bits of $P = P_0 + x$.

Two variables in $\mathbb{Z}$

$$p(x, y) = 1xy + Ax + By + C$$

$$\left[\begin{array}{cccc|ccccc}
C & . & . & . & 1 & * & * & * & * \\
A & C & . & . & x & * & * & * & * \\
. & A & . & . & x^2 & * & * & * & * \\
B & . & C & . & y & * & * & * & * \\
1 & B & A & C & xy & * & * & * & * \\
. & 1 & . & A & x^2y & * & * & * & * \\
. & . & B & . & y^2 & * & * & * & * \\
. & . & 1 & B & xy^2 & * & * & * & * \\
. & . & . & 1 & x^2y^2 & * & * & * & *
\end{array}\right]$$

- Solution $(x, y) \to$ vector $[1, x, x^2, y, xy, x^2y, y^2, xy^2, x^2y^2]^T$
- Orthogonal to vectors $[C, A, ., B, 1, ., ., ., .]^T \approx p(x, y)$
- $L =$ lattice of vectors $\approx x^i y^j p(x, y)$
- Build lattice M orthogonal to L
- Typical element $[m_*, m_x, m_{x^2}, m_y, mxy, m_{x^2y}, m_{y^2}, m_{xy^2}, m_{x^2y^2}]^T$ not necessarily $= [1, x, x^2, y, xy, x^2y, y^2, xy^2, x^2y^2]$ for some (x, y)
- Lattice basis reduction on M, find $(\dim(M) - 1)$ smallest basis elements

- Hyperplane equation defining the sublattice $M' \subset M$ spanned by them

- Small solution (x_0, y_0) (smaller than "determinant bound") will give an element of M' — can't involve largest basis element

- Equation of M' translates to polynomial equation $q(x_0, y_0) = 0$ not a multiple of $p(x, y)$

- Simultaneously solve $p(x, y) = q(x, y) = 0$ in $\mathbb{R}$

- Finds all small solutions (x_0, y_0).

Summary and extensions

Solve $p(x) = 0 \bmod N$ (univariate modular)

Solve $p(x, y) = 0 \in \mathbb{Z}$ (bivariate in $\mathbb{Z}$)

Can try same techniques for $p(x, y) = 0 \bmod N$ (bivariate modular) or $p(x, y, z) = 0 \in \mathbb{Z}$ (trivariate in $\mathbb{Z}$); not guaranteed to work but can sometimes.

(Boneh has done some applications on these lines.)

Return to One Variable mod N

Side effect of lattice proof: upper bound on number of small roots.

No more than dh roots x_0 with

$$|x_0| < B \approx N^{(h-1)/(dh-1)} \approx N^{(1/d)-(1/dh)}$$

Existential proof

An existential proof of this bound is due to
Konyagin & Steger, "On polynomial congruences" (1994).

$p(x) \bmod N$ has hd small roots x_a with $|x_a| < B/2$

Vandermonde matrix $M_1 = [x_a^j], 0 \leqslant a, j < hd$

$0 \neq |\det(M_1)| = \prod_{a<b} |x_a - x_b| < B^{(hd)(hd-1)/2}$

Row operations give matrix M_2 with entries $M_2 = [x_a^i p(x_a)^j], 0 \leqslant i < d, 0 \leqslant j < h$

Row of M_2 are divisible by N^j, so $\det(M_2)$ is divisible by $N^{dh(h-1)/2}$

Determinants are equal, so $N^{dh(h-1)/2} \leqslant B^{(hd)(hd-1)/2}$ and $B \geqslant N^{(h-1)/(hd-1)}$.

M_2 closely related to our matrix.

M_1 and M_2

$$M_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & x_4 & \cdots & x_{hd} \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 & \cdots & x_{hd}^2 \\ x_1^3 & x_2^3 & x_3^3 & x_4^3 & \cdots & x_{hd}^3 \\ & \vdots & & & \vdots & \\ x_1^j & x_2^j & x_3^j & x_4^j & \cdots & x_{hd}^j \\ & \vdots & & & \vdots & \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & x_4 & \cdots & x_{hd} \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 & \cdots & x_{hd}^2 \\ p(x_1) & p(x_2) & p(x_3) & p(x_4) & \cdots & p(x_{hd}) \\ x_1 p(x_1) & x_2 p(x_2) & x_3 p(x_3) & x_4 p(x_4) & \cdots & x_{hd} p(x_{hd}) \\ & \vdots & & & \vdots & \\ x_1^i p(x_1)^j & x_2^i p(x_2)^j & x_3^i p(x_3)^j & x_4^i p(x_4)^j & \cdots & x_{hd}^i p(x_{hd})^j \\ & \vdots & & & \vdots & \end{bmatrix}$$

Rows of M_2 are divisible by $(1, 1, 1, N, N, N, N^2, N^2, N^2, \ldots, N^{h-1}, N^{h-1})$

Relation of existential and constructive proofs:

Up to scaling of rows, our matrix L_3 and Konyagin and Steger's matrices M_1 and M_2 are related by

$$L_3 \times M_1 = M_2.$$

A second existential proof

Following H.W. Lenstra, “Divisors in residue classes”:
N squarefree, $N = \prod q_i$
k small roots $p(x_i) = 0 \bmod N$

$$-\frac{B}{2} < x_1 < x_2 < \cdots < x_k < +\frac{B}{2}$$

Define $Y = \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)$

$$0 < Y \leqslant B^{k(k-1)/2}$$

For each $q|N$, $p(x)$ has at most d different roots $\mod q$.
Number of pairs $(i < j, x_i = x_j \bmod q)$ is at least $d \times (\frac{k}{d})(\frac{k}{d} - 1)/2 = \frac{k(k-d)}{2d}$

(Worst case: k/d instances in each residue class):

$$q^{k(k-d)/2d} | Y$$

True for each $q|N$, and N is squarefree, so

$$N^{k(k-d)/2d} | Y$$

$$N^{k(k-d)/2d} \leqslant Y \leqslant B^{k(k-1)/2}$$
$$B \geqslant N^{(k-d)/(kd-d)}$$

Or, if $B < N^{(k-d)/(kd-d)}$ then number of roots is less than k.
Same bound as lattice construction.

Existential proof ...

Relaxing conditions:
"N squarefree": If $q^\ell | N, \ell > 1$, it suffices that $p(x)$ has d distinct roots $\mod q$. Hensel lifting gives $q | x_i - x_j \Rightarrow q^\ell | x_i - x_j$.

Example showing tightness

$$\begin{aligned} N &= q^3 \\ p(x) &= x^3 + aqx^2 + bq^2 x \end{aligned}$$

Any x with $q|x$ is a root: $p(x) = 0 \bmod N$.
If $B = N^{1/3+\epsilon}$ then there are N^ϵ roots with $|x| < B$ — exponentially many.

We do not know of other examples giving exponentially many roots.

Conjecture: If there are exponentially many roots x_i of $p(x) = 0 \bmod N$ with $|x_i| < B = N^{1/d+\epsilon}$, then N has a repeated prime factor $q^\ell|N$, and $p(x)$ has a repeated root mod q.

If so, then the discriminant of p is divisible by q, and we have:

$$\gcd\{N, Res_x[p(x), p'(x)]\} > 1$$

Also: If $q|N$, can't have more than deg(f) roots of $f(x) = 0 \bmod N$ smaller than q, since f has at most that many roots $\mathrm{mod} q$.

In RSA case, the polynomial has only one root $\mathrm{mod} N$, because of unique decryption.

Break up the hard case ($B = N^{1/3+\epsilon}$) into two hard problems:

(1) Show that the only bad examples are of this form
(so that $\gcd\{N, Res_x[p(x), p'(x)]\} > 1$)

(2) If not this bad case, use that (gcd=1) in the lattice solution:

$$\exists q(x), r(x) \in \mathbb{Z}[x]; c \in \mathbb{Z} :$$
$$q(x)p(x) + r(x)p'(x) + cN = 1$$

And then what?

Applications

- RSA, e=3, two related messages, difference $N^{1/9}$
- RSA, e=3, partially known message, unknown $N^{1/3}$
- Factor integers with partial information:

If $N = pq$, $p = N^{\alpha}$, know N and (approximately) α, with $p = p_0 + x$, known p_0, unknown $x < N^{\alpha^2}$, then can compute x.

- [Boneh] RSA with small decryption exponent

Known $N = pq$ and e. Unknown $p, q, \phi(N) = (p-1)(q-1) = N - s, d$

$$de = 1 + z\phi(N)$$
$$-1 + z(N - s) = 0 \bmod e$$

Unknown small z, s

• Divisors in residue classes (DC, Nick Howgrave-Graham):
H W Lenstra: Given $r, s, N \in \mathbb{Z}$ with $\gcd(r, s) = 1$ and $s > N^\alpha, \alpha > 1/4$,

$$\#\{d|N, d = r \bmod s\} < (\alpha - 1/4)^{-2} \text{ independent of } N$$

He showed this existentially for $\alpha > 1/4$ and constructively for $\alpha > 1/3$.
The present methods give constructively for $\alpha > 1/4$.

$$N - (xs + r)(ys + r') = 0, \quad x, y \text{ small}$$

• Primality testing: uses Lenstra's "divisors in residue classes" as subroutine

• Find worst cases for floating-point rounding of mathematical functions.
(Zimmerman, Stehle, Lefevre, 2003)

• "Some RSA-based Encryption Schemes with Tight Security Reduction"
(Kaoru Kurosawa and Tsuyoshi Takagi, IACR ePrint 2003-157)
Secret: p, q; Public: n, α, e; Secret nonce: $r < n$
Encryption: message $m < n \to$ ciphertext $c = (r + \frac{\alpha}{r})^e + mn) \bmod n^2$
Security reduction. Suppose we knew how to extract m from c.
— Choose random $\bar{r} < n$
— Compute $x = \bar{r} + \alpha/\bar{r} \bmod n^2$
— From fake random plaintext $\bar{m}$, compute ciphertext $c = x^e + \bar{m}n \bmod n^2$
— Obtain valid plaintext m from oracle
— Compute $w = c - mn = (r + \alpha/r)^e \bmod n^2$
— Compute $u = (w - x^e)/n$
— Compute $y = u/(ex^{e-1}) \bmod n$
— Compute $v = (\bar{r} + \alpha/\bar{r}) + ny \bmod n^2$
— Solve $r^2 - vr + \alpha = 0 \bmod n^2$ using present work

NP-hard variants

(Manders and Adleman) Given $\alpha, \beta, \gamma \in \mathbb{Z}$, it is NP-hard to decide whether there exist positive integers $\bar{x}, \bar{y}$ satisfying $\alpha\bar{x}^2 + \beta\bar{y} - \gamma = 0$. Remains NP-hard if factorization of β is known.

Easy to convert to NP-hard problem in our context:

Pick N sufficiently large, bounds $B_x = \sqrt{\gamma/\alpha}$ and $B_y = \gamma/2\beta$. Then it is NP-hard to decide whether there are solutions to

$$\alpha x^2 + \beta y - \tau = 0 \bmod N$$
$$|x| < B_x, \quad |y| < B_y$$

Bounds B_x, B_y do not grow with N.
Note: this is two variables mod N; we solve in one variable mod N.

Similarly

$$\alpha x^2 + \beta y - \tau - zN = 0$$
$$|x| < B_x, \quad |y| < B_y, \quad |z| < B_z = 2$$

This is in three variables over $\mathbb{Z}$; we solve in two variables over $\mathbb{Z}$.

Extensions

Divided difference for two different small roots

Univariate modular polynomial $p(x) = 0 \bmod N$, deg$(P) = d$.

Want two different small roots: $p(x) = p(y) = 0 \bmod N$,
$\gcd(x - y, N) = 1$

Cast as bivariate problem:

$$p(x) = 0, \quad p(y) = 0, \quad q(x, y) \equiv \frac{p(x) - p(y)}{x - y} = 0 \bmod N$$

The standard method can find x if $|x| < B_x = N^{1/d}$ or y if $|y| < B_y = N^{1/d}$. With the extra information (two different small roots), can find if

$$B_x^d B_y^{d-1} < N^2,$$

a slight improvement.

Conclusions

Find “small” solutions to “low” degree polynomials:

- In one variable mod N;
- In two variables over $\mathbb{Z}$.

Plenty of applications, mostly cryptographic.