J. Cryptol. (2013) 26: 246–250
DOI: 10.1007/s00145-012-9121-x

Journal of
CRYPTOLOGY

A Note on the Bivariate Coppersmith Theorem

Jean-Sébastien Coron
Université du Luxembourg, 6, rue Richard Coudenhove-Kalergi, 1359 Luxembourg, Luxembourg
jean-sebastien.coron@uni.lu

Alexey Kirichenko
F-Secure Corporation, Tammasaarenkatu 7, PL 24, 00181 Helsinki, Finland
alexey.kirichenko@f-secure.com

Mehdi Tibouchi
NTT Information Sharing Platform Laboratories, 3-9-1 Midori-cho, Musashino-shi, Tokyo 180-8585, Japan
tibouchi.mehdi@lab.ntt.co.jp

Communicated by Dan Boneh.

Received 15 June 2009
Online publication 21 March 2012

Abstract. In 1997, Coppersmith proved a famous theorem for finding small roots of bivariate polynomials over $\mathbb{Z}$, with important applications to cryptography.

While it seems to have been overlooked until now, we found the proof of the most commonly cited version of this theorem to be incomplete. Filling in the gap requires technical manipulations which we carry out in this paper.

Key words. Coppersmith's theorem, Bivariate polynomials, Small roots.

1. Introduction

In his seminal 1997 paper [1], Coppersmith shows how to find small roots of polynomials mod N, as well as bivariate polynomials over the integers. In particular, he proves the following theorem:

Theorem 1 (Coppersmith [1, Theorem 2]). *Let $p(x, y)$ be an irreducible polynomial in two variables over $\mathbb{Z}$, of maximum degree δ in each variable. Let X, Y be bounds on the desired solutions x_0, y_0. Define $\tilde{p}(x, y) = p(xX, yY)$ and let W be the supremum of the absolute values of the coefficients of $\tilde{p}$. If, for some $\varepsilon > 0$,*

$$XY < W^{2/(3\delta)-\varepsilon} 2^{-14\delta/3} \tag{1}$$

then in time polynomial in $(\log W, 2^{\delta}, 1/\varepsilon)$, we can find all integer pairs (x_0, y_0) with $p(x_0, y_0) = 0$, $|x_0| < X$ and $|y_0| < Y$.

From this, he deduces a widely cited corollary:

Corollary 1 ([1, Corollary 2]). *With the hypothesis of Theorem 1, except that*

$$XY \leq W^{2/(3\delta)}$$

then in time polynomial in $(\log W, 2^{\delta})$, *we can find all integer pairs* (x_0, y_0) *with* $p(x_0, y_0) = 0$, $|x_0| \leq X$ *and* $|y_0| \leq Y$.

For Corollary 1 the following proof is given in [1]: "Set $\varepsilon = 1/\log W$, and do exhaustive search on the high-order $O(\delta)$ unknown bits of x. The running time is still polynomial, but of higher degree in $(\log W)$."

However, we claim that this proof is incomplete. Carrying out an exhaustive search on the ℓ highest-order bits of x_0 essentially amounts to writing:

$$x_0 = 2^{-\ell}\alpha X + x_0'$$

where X is assumed to be a multiple of 2^{ℓ} and $|x_0'| < 2^{-\ell}X$, and to doing exhaustive search on α for $|\alpha| \leq 2^{\ell}$. We are thus looking for a solution (x_0', y_0) of the polynomial equation $q(x, y) = 0$ given by

$$q(x, y) := p\big(2^{-\ell}\alpha X + x, y\big) \tag{2}$$

where x_0' is now bounded in absolute value by $X' = 2^{-\ell}X$ instead of X. Then, in order to apply Theorem 1 for the polynomial $q(x, y)$, one must consider the new bound for q:

$$W_q = \max_{ij} \left| q_{ij} X'^i Y^j \right|,$$

instead of the original bound $W = \max_{ij} |p_{ij} X^i Y^j|$. However it is *a priori* unclear whether condition (1) will be satisfied for X', Y, and W_q. Namely, the coefficients of $q(x, y)$ could become very small because of the change of variable in (2), and W_q might then be too small for condition (1) to be satisfied. What we show is that this does not in fact happen: W_q can be bounded appropriately so that condition (1) holds for q as well (technically, we show this when exhaustive search is carried out on ℓ bits of *both* x and y, hence with a polynomial slightly different from q; the argument adapts to q as well, however).

Note that this problem does not occur in the univariate case modulo N, since in that case the condition on X only depends on the modulus N and not on the coefficients of the polynomial.

The gap is also present in other works building upon [1], such as [2,3], and the fix we propose here applies to those other papers as well.

2. A Proof of Corollary 1

In order to prove Corollary 1, we do exhaustive search on ℓ bits of both x and y, which is similar to the above but somewhat more symmetric. This amounts to writing

$$x_0 = 2^{-\ell}\alpha X + x_0', \qquad y_0 = 2^{-\ell}\beta Y + y_0'$$

and applying Theorem 1 to polynomials p' of the form

$$p'(x, y) = p\big(x + 2^{-\ell}\alpha X, y + 2^{-\ell}\beta Y\big)$$

with $|\alpha|, |\beta| \leq 2^{\ell}$, and x'_0 and y'_0 now bounded in absolute value by $X' = 2^{-\ell}X$ and $Y' = 2^{-\ell}Y$, respectively; here we assume wlog that X and Y are multiples of 2^{ℓ}. In order to check that the hypotheses of the theorem do indeed hold, we need to estimate the supremum W' of absolute value of the coefficients of $\tilde{p}'(x, y) = p'(xX', yY')$.

Lemma 1. *The constant W' satisfies*

$$2^{-2\delta(\ell+2\delta+4)-1} W \leq W' \leq 16^{\delta} W.$$

Proof. We first compute the coefficients of $\tilde{p}'$. For all indices a, b:

$$p'_{ab} = \sum_{i=a}^{\delta}\sum_{j=b}^{\delta} \binom{i}{a}\binom{j}{b} p_{ij} \left(\frac{\alpha X}{2^{\ell}}\right)^{i-a} \left(\frac{\beta Y}{2^{\ell}}\right)^{j-b},$$

$$\tilde{p}'_{ab} = X'^{a} Y'^{b} \sum_{i=a}^{\delta}\sum_{j=b}^{\delta} \binom{i}{a}\binom{j}{b} \frac{\tilde{p}_{ij}}{X^i Y^j} \left(\frac{\alpha X}{2^{\ell}}\right)^{i-a} \left(\frac{\beta Y}{2^{\ell}}\right)^{j-b},$$

$$\tilde{p}'_{ab} = 2^{-(a+b)\ell} \sum_{i=a}^{\delta}\sum_{j=b}^{\delta} \binom{i}{a}\binom{j}{b} \tilde{p}_{ij} \left(\frac{\alpha}{2^{\ell}}\right)^{i-a} \left(\frac{\beta}{2^{\ell}}\right)^{j-b}.$$

Using crude bounds, it follows that

$$\big|\tilde{p}'_{ab}\big| \leq 1 \times \sum_{i=a}^{\delta}\sum_{j=b}^{\delta} 2^{\delta} \cdot 2^{\delta} \cdot W \cdot 1 \cdot 1 \leq (\delta+1)^2 \cdot 4^{\delta} \cdot W \leq 16^{\delta} W,$$

which is the required upper bound.

Turning to the lower bound, let λ be a real number > 2 which will be chosen later. We then let (c, d) denote a pair of indices such that $\lambda^{c+d}|\tilde{p}_{cd}|$ is maximal. This maximum will be denoted W_{λ}. We have

$$\tilde{p}'_{cd} = 2^{-(c+d)\ell}\left[\tilde{p}_{cd} + \sum_{\substack{c\leq i\leq\delta \\ d\leq j\leq\delta \\ (i,j)\neq(c,d)}} \binom{i}{c}\binom{j}{d} \tilde{p}_{ij} \left(\frac{\alpha}{2^{\ell}}\right)^{i-c} \left(\frac{\beta}{2^{\ell}}\right)^{j-d}\right].$$

Note further that, since $\lambda^{i+j}|\tilde{p}_{ij}|$ is maximal for $(i, j) = (c, d)$,

$$\big|\tilde{p}_{ij}\big| \leq \lambda^{(c-i)+(d-j)}|\tilde{p}_{cd}| \quad \text{for all } i, j.$$

We can thus bound the terms in the last sum as follows:

$$\left|\binom{i}{c}\binom{j}{d}\tilde{p}_{ij}\left(\frac{\alpha}{2^\ell}\right)^{i-c}\left(\frac{\beta}{2^\ell}\right)^{j-d}\right| \le 2^i \cdot 2^j \cdot \lambda^{(c-i)+(d-j)}\left|\tilde{p}_{cd}\right| \cdot 1 \cdot 1$$
$$\le 4^\delta \left|\tilde{p}_{cd}\right| \cdot \lambda^{(c-i)+(d-j)}.$$

This entails that $\tilde{p}'_{cd}$ is lower bounded in absolute value as

$$\left|\tilde{p}'_{cd}\right| \ge 2^{-(c+d)\ell}|\tilde{p}_{cd}|\left[1 - 4^\delta \sum_{\substack{c\le i\le\delta \\ d\le j\le\delta \\ (i,j)\neq(c,d)}} \lambda^{(c-i)+(d-j)}\right].$$

Now we write

$$\sum_{\substack{c\le i\le\delta \\ d\le j\le\delta \\ (i,j)\neq(c,d)}} \lambda^{(c-i)+(d-j)} \le \sum_{\substack{x,y\ge 0 \\ (x,y)\neq(0,0)}} \lambda^{-x-y} = \frac{1}{(1-1/\lambda)^2} - 1 = \frac{2/\lambda - 1/\lambda^2}{(1-1/\lambda)^2} \le \frac{8}{\lambda}$$

since we chose $\lambda \ge 2$. Plugging this into the previous inequality, we obtain

$$\left|\tilde{p}'_{cd}\right| \ge 2^{-(c+d)\ell}|\tilde{p}_{cd}|\left(1 - 4^\delta \cdot \frac{8}{\lambda}\right) \ge 2^{-(c+d)\ell-1}\left|\tilde{p}_{cd}\right|$$

if we pick $\lambda = 4^{\delta+2}$. Then, observing that $W' \ge |\tilde{p}'_{cd}|$ by maximality, and $|\tilde{p}_{cd}| = \lambda^{-c-d}W_\lambda \ge \lambda^{-c-d}W$ by definition of c and d, we get

$$W' \ge 2^{-(c+d)\ell-1} \cdot 4^{-(c+d)(\delta+2)}W \ge 2^{-2\delta(\ell+2\delta+4)-1}W$$

as required. □

Lemma 2. *Under the hypothesis of Corollary 1, namely $XY \le W^{2/(3\delta)}$, the following inequality holds for $\varepsilon = 1/\log_2 W$ and some large enough $\ell = O(\delta)$:*

$$X'Y' \le \left(W'\right)^{2/(3\delta)-\varepsilon}2^{-14\delta/3}.$$

Proof. Note first that

$$\begin{aligned} X'Y' &\le 2^{-2\ell}XY \\ &\le 2^{-2\ell}W^{2/(3\delta)} \\ &\le 2^{-2\ell}\left(2^{2\delta(\ell+2\delta+4)+1}W'\right)^{2/(3\delta)} \\ &\le 2^{-2\ell/3+8\delta/3+16/3+2/(3\delta)}\left(W'\right)^{2/(3\delta)} \\ &\le 2^{-2\ell/3+22\delta/3+6}\left(W'\right)^{\varepsilon} \cdot \left(W'\right)^{2/(3\delta)-\varepsilon}2^{-14\delta/3}. \end{aligned}$$

Hence, it suffices to show that the logarithm of the first factor

$$L = \log_2\left(2^{-2\ell/3+22\delta/3+6}\left(W'\right)^{\varepsilon}\right)$$

is negative for some suitable $\ell = O(\delta)$. We have

$$\begin{aligned} L &= -\frac{2}{3}\ell + \frac{22}{3}\delta + 6 + \varepsilon \log_2 W' \\ &\leq -\frac{2}{3}\ell + \frac{22}{3}\delta + 6 + \varepsilon \log_2\left(16^{\delta} W\right) \\ &= -\frac{2}{3}\ell + \frac{22}{3}\delta + 6 + \varepsilon \cdot (4\delta + \log_2 W) \\ &\leq -\frac{2}{3}\ell + \frac{34}{3}\delta + 7, \end{aligned}$$

since, without loss of generality, $\varepsilon \leq 1$. Thus, picking any $\ell > 17\delta + 11$ gives the required inequality. □

Corollary 1 is easily deduced from Lemma 2. Indeed, exhaustive search requires $(2^{\ell+1}+1)^2$ applications of Theorem 1 (taking into account all positive, negative and zero values of α and β), each of which runs in time polynomial in $(\log W, 2^{\delta})$. Since $\ell = O(\delta)$, the whole computation runs in time polynomial in $(\log W, 2^{\delta})$ as well.

Note that the bound on ℓ is very coarse, as we did not want to make the computation more cumbersome by using tighter inequalities. In practice, however, one could of course get away with far fewer bits of exhaustive search.

References

[1] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.* **10**(4), 233–260 (1997)

[2] J.-S. Coron, Finding small roots of bivariate integer polynomial equations revisited, in *Proceedings of Eurocrypt 2004*. LNCS, vol. 3027 (Springer, Berlin, 2004), pp. 492–505

[3] J.-S. Coron, Finding small roots of bivariate integer polynomial equations: a direct approach, in *Proceedings of CRYPTO 2007*. LNCS, vol. 4622 (Springer, Berlin, 2007), pp. 379–394