Seminar Notes (09/16/05): *The factorization of x^2+x revisited, Part I*
(joint work with M. A. Bennett and O. Trifonov)

Notation:

$$x_0 = (D\mathcal{M}_2^c)^{\frac{M+1}{1-\lambda}}, \quad \mathcal{D} = \frac{\log D}{c\log \mathcal{M}_2} + 1, \quad c > d \geq 1 \ (c, d \in \mathbb{Z}), \quad t \in (0,1)$$

$$M = \max\left\{ \frac{\log(\kappa_1)}{d\,\mathcal{D}\,\log\Omega_3}, \frac{\log\left(\mathcal{M}_2^c\,\kappa_2^{-1}\right)}{\epsilon\,d\,\mathcal{D}\,t\,\log(\mathcal{M}_2^s\,\Omega_4)}, \frac{\lambda\,\log(\kappa_2 D)}{\epsilon\,d\,\mathcal{D}\,(1-t)\,\log(\mathcal{M}_2^s\,\Omega_4)}, \frac{m_0}{\mathcal{D}} \right\}.$$

Notation for Later: $\Omega_3 = \Omega_3(s)$, $\Omega_4 = \Omega_4(s)$, κ_1, κ_2

Theorem 1. *Let p and q be distinct primes. Suppose that there exist positive integers a, b, k_0, l_0 and D_0 such that*

$$ap^{k_0} - bq^{l_0} = D_0,$$

and write

$$z_0 = D_0/(ap^{k_0}), \ \mathcal{M}_1 = \min\{p^{k_0}, q^{l_0}\} \ \text{ and } \ \mathcal{M}_2 = \max\{p^{k_0}, q^{l_0}\}.$$

Assume further that there exists a rational number s satisfying $1 < s < 1/z_0$, $\Omega_3 > 1$ and $\Omega_4 > 1$. Set $\lambda = \log(\Omega_4)/\log(\mathcal{M}_2^s\,\Omega_4)$. Let D be a positive integer, and fix $\epsilon > 0$. Define x_0 as above. If $x \geq x_0$ is an integer and

$$x^2 + Dx = p^k q^l y$$

with k, l, and y nonnegative integers, then $y \geq x^{\lambda-\epsilon}$.

Corollary 1. *Let p, q and $\lambda = \lambda(p,q)$ be as in the table below.*

p	q	$\lambda(p,q)$	p	q	$\lambda(p,q)$
2	3	0.27	3	11	0.32
2	5	0.25	5	11	0.19
3	5	0.21	2	13	0.05
2	7	0.25	3	13	0.22
3	7	0.03	5	13	0.16
5	7	0.22	7	13	0.09
2	11	0.05	11	13	0.03

Let D be an integer satisfying $1 \leq D \leq 100$. Then, if we write

$$x^2 + Dx = p^k q^l y,$$

for k, l and y nonnegative integers, we have $y \geq x^\lambda$, unless $x \leq 1000$ or (p,q,x,D) is in the set

$$\{(2,3,32768,37), (2,3,65536,74), (2,3,1458,78), (2,5,3072,53),$$
$$(2,7,1024,5), (2,7,2048,10), (5,7,2401,99), (3,11,14580,61),$$
$$(3,11,1771470,91), (3,11,6561,94), (5,11,1250,81), (3,13,2187,10),$$
$$(3,13,4374,20), (3,13,6561,30)\}.$$

Definition (or Lemma): For positive integers A, B and C, define

$$P_{A,B,C}(z) = \sum_{r=0}^{C} \binom{A+B+C+1}{r} \binom{A+C-r}{A} (-z)^r,$$

$$Q_{A,B,C}(z) = (-1)^C \sum_{r=0}^{A} \binom{A+C-r}{C} \binom{B+r}{r} z^r$$

and

$$E_{A,B,C}(z) = \sum_{r=0}^{B} \binom{A+r}{r} \binom{A+B+C+1}{A+C+r+1} (-z)^r.$$

Lemma 1. *The polynomials above satisfy*

$$P_{A,B,C}(z) - (1-z)^{B+C+1} Q_{A,B,C}(z) = z^{A+C+1} E_{A,B,C}(z).$$

Lemma 2. *There is a non-zero integer $D = D(A,B)$ for which*

$$P_{A,B,A}(z) Q_{A+1,B-1,A+1}(z) - Q_{A,B,A}(z) P_{A+1,B-1,A+1}(z) = D z^{2A+1}.$$

Proof of Theorem 1 (Part I):

• Note it suffices to consider $\gcd(y, pq) = 1$.

• Define $D_1 = \gcd(x, x+D) = p^{\alpha} q^{\beta} y_0$ with $\gcd(pq, y_0) = 1$. Observe that x/D_1 and $(x+D)/D_1$ are relatively prime with product $p^{k-2\alpha} q^{l-2\beta} y/y_0^2$. If either x/D_1 or $(x+D)/D_1$ is coprime to pq, then $y/y_0^2 \geq x/D_1$ so that $y \geq x/D$. In this case, $\lambda < 1$ and $x \geq D^{1/(1-\lambda)}$ imply $y \geq x^{\lambda}$. Therefore, we can suppose p divides $(x+D)/D_1$ and q divides x/D_1 (or something like that).

• Set $D_2 = D/D_1$. Then $D_2 = p^{k-2\alpha} y_1 - q^{l-2\beta} y_2$, where $y = y_0^2 y_1 y_2$. We will show y_1 or y_2 is $\geq x^{\lambda-\epsilon}$.

• Write $s = c/d$ with $\gcd(c,d) = 1$. Take m_1, m_2, $0 \leq \alpha_1 < k_0 c$ and $0 \leq \beta_1 < l_0 c$ integers satisfying $k - 2\alpha = k_0 c m_1 + \alpha_1$ and $l - 2\beta = l_0 c m_2 + \beta_1$. Set $y_1' = p^{\alpha_1} y_1$ and $y_2' = q^{\beta_1} y_2$. Then $D_2 = p^{k_0 c m_1} y_1' - q^{l_0 c m_2} y_2'$.

• Take $m = \min\{m_1, m_2\}$. Then

$$D_2 = p^{k_0 c m} y_1'' - q^{l_0 c m} y_2'' \tag{1}$$

where either $y_1'' = y_1'$ or $y_2'' = y_2'$ and $y \geq \min\{p^{-\alpha_1} y_1'', q^{-\beta_1} y_2''\}$.

• Take $n = dm - \delta$ where $\delta \in \{0,1\}$. Let $A = C = n$ and $B = cm - n - 1$. Let $P_n(z)$, $Q_n(z)$, and $E_n(z)$ denote the polynomials in the definition above, and set $\mathcal{G} = \mathcal{G}(c,d,n)$ to be the gcd of the coefficients of $Q_n(z)$. Lemma 1 implies then that $P_n(z)/\mathcal{G}$, $Q_n(z)/\mathcal{G}$, and $E_n(z)/\mathcal{G}$ have integer coefficients.

• Use $z = z_0$ in Lemma 1 to deduce

$$\left(ap^{k_0}\right)^{cm} P - \left(bq^{\ell_0}\right)^{cm} Q = E \tag{2}$$

where P, Q and E are integers defined by

$$P = (ap^{k_0})^n P_n(z_0)/\mathcal{G}, \quad Q = (ap^{k_0})^n Q_n(z_0)/\mathcal{G}, \quad \text{and} \quad E = (ap^{k_0})^{cm-n-1} D_0^{2n+1} E_n(z_0)/\mathcal{G}.$$

• Multiplying (1) by $b^{cm} Q$ and (2) by y_2'', we deduce that

$$p^{k_0 cm} \left| b^{cm} Q y_1'' - a^{cm} P y_2'' \right| \leq b^{cm} D |Q| + |E| y_2''.$$

• Lemma 2 implies that the expression $b^{cm} Q y_1'' - a^{cm} P y_2''$ is nonzero for at least one of $n = dm$ and $n = dm - 1$. Fix δ accordingly. Then $p^{k_0 cm} \leq b^{cm} D |Q| + |E| y_2''$. The idea is to show that $|Q|$ and $|E|$ are not too large and deduce a lower bound on y_2''.

• If $y < x^{\lambda}$, then $\min\{p^{-\alpha_1} y_1'', q^{-\beta_1} y_2''\} < x^{\lambda}$ so that either

$$x = D_1 q^{l_0 cm} y_2'' = D_1 q^{l_0 cm} q^{\beta_1} q^{-\beta_1} y_2'' < D q^{l_0 cm} q^{l_0 c} x^{\lambda} \quad \Longrightarrow \quad q^{l_0 cm} > x^{1-\lambda} / \left(D q^{l_0 c}\right)$$

or, similarly from $x+D=D_1p^{k_0cm}y_1''$, we have $p^{k_0cm}>x^{1-\lambda}/\big(Dp^{k_0c}\big)$. Therefore,

$$m>\min\left\{\frac{(1-\lambda)\log x-\log\big(Dq^{l_0c}\big)}{\log\left(q^{l_0c}\right)},\frac{(1-\lambda)\log x-\log\big(Dp^{k_0c}\big)}{\log\left(p^{k_0c}\right)}\right\}.$$

The condition $x\geq x_0$ implies

$$(1-\lambda)\log x\geq(M+1)\log\big(D\mathcal{M}_2^c\big)\geq M\log\big(D\mathcal{M}_2^c\big)+\max\big\{\log\big(Dp^{k_0c}\big),\log\big(Dq^{l_0c}\big)\big\}.$$

Hence, $m>M\log\big(D\mathcal{M}_2^c\big)/\max\big\{\log(q^{l_0c}),\log(p^{k_0c})\big\}=M\log\big(D\mathcal{M}_2^c\big)/\log(\mathcal{M}_2^c)=M\mathcal{D}$. It follows that

$$dm>\max\left\{\frac{\log\left(\kappa_1\right)}{\log\Omega_3},\frac{\log\left(\mathcal{M}_2^c\,\kappa_2^{-1}\right)}{\epsilon\,t\,\log\left(\mathcal{M}_2^s\,\Omega_4\right)},\frac{\lambda\log(\kappa_2D)}{\epsilon\,(1-t)\,\log\left(\mathcal{M}_2^s\,\Omega_4\right)},dm_0\right\}.$$