Seminar Notes (09/23/05): *The factorization of x^2+x revisited, Part II*
(joint work with M. A. Bennett and O. Trifonov)

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

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

$$\Omega_3 = \frac{p^{k_0(s-1)}\,L_1(s)}{ab^s\,Q(s,z_0)}, \quad \Omega_4 = \frac{\mathcal{M}_1^s\,L_1(s)}{(ap^{k_0})^{s-1}\,D_0^2\,E(s,z_0)}, \quad \kappa_1 = \max_{\delta\in\{0,1\}} \frac{2\,D\,C_{1,\delta}}{(ap^{k_0})^{\delta}}, \quad \kappa_2 = \min_{\delta\in\{0,1\}} \frac{(ap^{k_0})^{1-\delta}}{2D_0^{1-2\delta}C_{2,\delta}}$$

The undefined notation: The expressions $Q(s,z)$, $E(s,z)$, $C_{1,\delta}$, $C_{2,\delta}$ come from Lemma 3 below (bounds on $|Q_n(z)|$ and $|E_n(z)|$, themselves defined in the proof). Also, $L_1(s)$ comes from a bound on $\mathcal{G}(c,d,n)$; specifically, $\mathcal{G}(c,d,n) \geq L_1(s)^{dm}$ for $m > m_0$.

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 $y \geq x^{\lambda-\epsilon}$.

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

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

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*

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

Lemma 3. *If $n = dm - \delta$ for $\delta \in \{0,1\}$, then*

$$\left|Q_n(z)\right| < C_{1,\delta}\big(Q(s,z)\big)^{dm} \qquad \text{and} \qquad \left|E_n(z)\right| < C_{2,\delta}\big(E(s,z)\big)^{dm}.$$

Proof of Theorem 1 (Part II):

• Recall that with $(x+D)/D_1 = p^{k_0 cm} y_1''$ and $x/D_1 = q^{l_0 cm} y_2''$, we reduced the problem to considering

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

where $D_2 = D/D_1$, $D_1 = \gcd(x, x+D)$, $y \geq \min\{p^{-\alpha_1} y_1'', q^{-\beta_1} y_2''\}$, $0 \leq \alpha_1 < k_0 c$ and $0 \leq \beta_1 < l_0 c$.

• 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''.

• We show later (at the end of these notes) that if $y < x^\lambda$, then

$$dm > \max\left\{\frac{\log(\kappa_1)}{\log \Omega_3}, \frac{\log\left(\mathcal{M}_2^c \kappa_2^{-1}\right)}{\epsilon\, t \log\left(\mathcal{M}_2^s \Omega_4\right)}, \frac{\lambda \log(\kappa_2 D)}{\epsilon\,(1-t) \log\left(\mathcal{M}_2^s \Omega_4\right)}, dm_0\right\}. \tag{3}$$

• Using the definition of Q and the lower bound on $\mathcal{G}$, we have

$$|Q| < \frac{(ap^{k_0})^{dm-\delta} C_{1,\delta} Q(s,z_0)^{dm}}{L_1(s)^{dm}} \leq \frac{\kappa_1}{2D}\left(\frac{ap^{k_0} Q(s,z_0)}{L_1(s)}\right)^{dm}.$$

• From (3), $\kappa_1 < \Omega_3^{dm}$. The definition of Ω_3 and $p^{k_0 cm} \leq b^{cm} D|Q| + |E| y_2''$ imply $y_2'' > p^{k_0 cm}/(2|E|)$.

• Note that $|E| < \left((ap^{k_0})^{(c-d)m+\delta-1} D_0^{2dm+1-2\delta} C_{2,\delta} E(s,z_0)^{dm}\right)/L_1(s)^{dm}$ implies

$$y_2'' > \kappa_2 \left(\frac{p^{k_0} L_1(s)}{a^{s-1} D_0^2 E(s,z_0)}\right)^{dm} = \kappa_2 \Omega_4^{dm}\left(\frac{p^{k_0}}{\mathcal{M}_1}\right)^{cm} \geq \kappa_2 \Omega_4^{dm}.$$

• From (1), $y_1'' \geq (q^{l_0}/p^{k_0})^{cm} y_2'' > \kappa_2 \Omega_4^{dm} (q^{l_0}/\mathcal{M}_1)^{cm} \geq \kappa_2 \Omega_4^{dm}$.

• Since $y \geq \min\{p^{-\alpha_1} y_1'', q^{-\beta_1} y_2''\} \geq \mathcal{M}_2^{-c} \min\{y_1'', y_2''\}$, we deduce $\log y \geq -\log(\mathcal{M}_2^c) + \min\{\log y_1'', \log y_2''\}$.

• From $x = D_1 q^{l_0 cm} y_2'' \leq D_1 p^{k_0 cm} y_1''$ and $D_1 \leq D$, we have $\log x \leq \log D + dm \log(\mathcal{M}_2^s) + \min\{\log y_1'', \log y_2''\}$.

• If u and v are positive numbers, then the function $(w-u)/(w+v)$ is increasing. It follows that

$$\frac{\log y}{\log x} \geq \frac{-\log(\mathcal{M}_2^c) + \min\{\log y_1'', \log y_2''\}}{\log D + dm \log(\mathcal{M}_2^s) + \min\{\log y_1'', \log y_2''\}} > \frac{-\log(\mathcal{M}_2^c) + \log\left(\kappa_2 \Omega_4^{dm}\right)}{\log D + dm \log(\mathcal{M}_2^s) + \log\left(\kappa_2 \Omega_4^{dm}\right)}.$$

• Hence, $y \geq x^\theta$ where $\theta = \dfrac{\log(\Omega_4) - \log\left(\mathcal{M}_2^c \kappa_2^{-1}\right)/(dm)}{\log\left(\mathcal{M}_2^s \Omega_4\right) + \log(\kappa_2 D)/(dm)}$.

• With a little effort, one checks that $\theta > \lambda - \epsilon$ follows from (3). Indeed, this is how M was chosen.

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

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

or, similarly from $x + D = D_1 p^{k_0 cm} y_1''$, we have $p^{k_0 cm} > x^{1-\lambda} / \big(D p^{k_0 c}\big)$. Therefore,

$$m > \min\left\{ \frac{(1-\lambda)\log x - \log\big(D q^{l_0 c}\big)}{\log\left(q^{l_0 c}\right)}, \frac{(1-\lambda)\log x - \log\big(D p^{k_0 c}\big)}{\log\left(p^{k_0 c}\right)} \right\}.$$

The condition $x \geq x_0$ implies

$$(1-\lambda)\log x \geq (M+1)\log\big(D\mathcal{M}_2^c\big) \geq M\log\big(D\mathcal{M}_2^c\big) + \max\big\{\log\big(D p^{k_0 c}\big), \log\big(D q^{l_0 c}\big)\big\}.$$

Hence, $m > M\log\big(D\mathcal{M}_2^c\big) / \max\big\{\log(q^{l_0 c}), \log(p^{k_0 c})\big\} = M\log\big(D\mathcal{M}_2^c\big) / \log(\mathcal{M}_2^c) = M\mathcal{D}$. It follows that

$$dm > \max\left\{ \frac{\log(\kappa_1)}{\log\Omega_3}, \frac{\log\left(\mathcal{M}_2^c \,\kappa_2^{-1}\right)}{\epsilon\, t\, \log\left(\mathcal{M}_2^s\,\Omega_4\right)}, \frac{\lambda\log(\kappa_2 D)}{\epsilon\,(1-t)\,\log\left(\mathcal{M}_2^s\,\Omega_4\right)}, dm_0 \right\}. \tag{4}$$