SERMON (South East Regional Meeting On Numbers)

April 17 - 18, 1999

University of South Carolina
Columbia, South Carolina, United States

A search for new factorial and primorial primes

Chris K. Caldwell
University of Tennessee at Martin

We report on a search for the primes of the forms $2 \cdot 3 \cdot \ldots \cdot p \pm 1$ (the primorial primes) up to $p = 100000$, and $n! \pm 1$ (the factorial primes) up to $n = 10000$. We then do a heuristical analysis to suggest a possible distribution of primes of these forms and call into question the fact that we found only three new primes in these ranges.

Joint work with Yves Gallot (de l'Ecole Suprieure d'Electricit)

`caldwell@utm.edu`

New Results in Egyptian Fractions

Ernie Croot
The University of Georgia

This talk will be a survey of results in the theory of Egyptian Fractions, including recent results by myself and by Greg Martin. One such result is that given any rational $r > 0$, and for any $N > 1$, there exist integers $n_1, ..., n_k$, k variable, such that

$$N \leq n_1 < n_2 < \cdots < n_k \leq (e^r + O_r(\log\log N / \log N))\, N,$$

and

$$r = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}.$$

Moreover, the error term $O_r(\log\log N / \log N)$ is best-possible. This result answers several questions posed by Erdos, R. Graham, and others.

`ecroot@alpha.math.uga.edu`

Spectra of Heights over Finite Groups.

Greg Dresden
Washington & Lee University

The (Weil) height of an algebraic number, $h(\alpha)$, is related to the Mahler measure of its minimal polynomial $p_\alpha(x)$ as follows: $h(\alpha) = \frac{1}{\deg p_\alpha} \log M(p_\alpha)$. While $h(\alpha)$ is clearly dense in $[0, \infty)$ as α ranges over all algebraic numbers, Zhang showed that $h(\alpha)+h(1-\alpha)$ is (at first) discrete. We expand this to other sums of heights of algebraic numbers, taking advantage of the group structure and of C. Smyth's recent work on discreteness and density of $h(\alpha)$ for α totally real.

`dresdeng@wlu.edu`

From Covering Problems to a Conjecture of Turan

Michael Filaseta
University of South Carolina

A covering of the integers is a system of congruences $x \equiv a_j \pmod{m_j}$, where a_j and m_j denote integers with $m_j > 0$ for each j, such that every integer satisfies at least one of the congruences. A conjecture of Turán's asserts loosely that every polynomial with integer coefficients is close to an irreducible polynomial with integer coefficients. More precisely, he has conjectured that there is an absolute constant C such that if $f(x) = \sum_{j=0}^{r} a_j x^j$ has integral coefficients, then there is an irreducible $g(x) = \sum_{j=0}^{s} b_j x^j$ with integer coefficients such that $s \leq r$ and such that the sum of the absolute values of the coefficients of $f(x) - g(x)$ is bounded by C. The conjecture remains open, though Schinzel has established the conjecture with the condition $s \leq r$ replaced by a more relaxed condition on s. This talk will be a survey of some recent investigations beginning with some old results and questions on coverings, moving to connected questions about polynomials and their reducibility, and ending with some recent progress on the conjecture of Turán.

`filaseta@math.sc.edu`

New results in comparative prime number theory

Kevin Ford
University of South Carolina

Let $\pi(q,a;x)$ denote the number of prime numbers $\le x$ and lying in the progression a modulo q. Set $\Delta(q,a,b;x) = \pi(q,a;x) - \pi(q,b;x)$. The study of the behavior of the functions $\Delta(q,a,b;x)$ has been termed "comparative prime number theory". We present some new results, both theoretical and computational, concerning the location of sign changes of $\Delta(q,a,b;x)$ for general q, and give some specifics in the case $q = 8$.

Joint work with Richard Hudson

ford@math.sc.edu

On distribution of integers with missing digits in residue classes

Sergei Konyagin
Moscow State University

Let

$$g \in \mathbf{N}, \quad g \ge 3, \quad t \in \mathbf{N}, \quad 2 \le t \le g-1, \tag{1}$$

$$D \subset \{0, 1, \ldots, g-1\}, \quad 0 \in D, \quad |D| = t, \tag{2}$$

and let $W_D(N)$ denote the set of integers n such that $0 \le n \le N$ and representing n in the number system to base g:

$$n = \sum_{j=0}^{\nu} a_j g^j, \quad 0 \le a_j \le g-1,$$

where $g^\nu \le N < g^{\nu+1}$, we have $a_j \in D$ for $j = 0, \ldots, \nu$. P. Erdös, C. Mauduit and A. Sárközy [1] proved, among many other interesting results, that the set $W_D(N)$ is well-distributed in the modulo m residue classes if $m < \exp(c(g,t)(\log N)^{1/2})$. Also, they showed that if $t > g^{3/4}$, a positive integer z is small enough in terms of t and g (namely, $z < (2(1-\log t/\log g))^{-1}$), then $W_D(N)$ contains integers with zth power parts as large as cN^c with $c = c(g,t,z) > 0$. It turns out that the last property holds for all g, t and z.

Theorem 1 If g and t satisfy (1), (2) holds, and writing $D = \{d_1, \ldots, d_s\}$ where $d_1 = 0$, we have $(d_2, \ldots, d_t) = 1$, moreover, $\nu \in \mathbf{N}$, $N = g^\nu$, $\mu \in \mathbf{N}$, $M = g^\mu$, $L \in \mathbf{N}$, $m_1, \ldots, m_L$ are pairwise relatively prime distinct positive integers such that for any $j \in \{1, \ldots, L\}$ we have $m_j < M$, $(g, m_j) = 1$, and $W_D(N)$ does not meet some residue class modulo m_j, then

$$L \le \left(1 + g\left(1 - \frac{1}{(g-1)^5(2g)^2}\right)^{[\nu/\mu]}\right)^{2\mu} - 1.$$

Corollary Let the conditions (1) and (2) be satisfied. Then there exist effectively computable positive constants $c_1(g) > 0$ and $c_2(g) > 0$ such that if $z \geq 2$ is a postitive integer and $N \geq z^{c_1(g)z}$, then there are $n \in W_D(N)$ and prime p such that $n > 0$, $p > N^{c_2(g)/(z \log z)}$ and $p^z | n$.

Theorem 2 If g and t satisfy (1), then there exist effectively computable positive constant $c_1(g) > 0$, $c_2(g) > 0$, $c_3(g) > 0$ such that if also (2) holds, and writing $D = \{d_1, \dots, d_s\}$ where $d_1 = 0$, we have $(d_2, \dots, d_t) = 1$, moreover, $N \in \mathbf{N}$, $N \geq 2$, $m \in \mathbf{N}$, $m \geq 2$, $(g, m) = 1$, $m < \exp(c_1 \log N / \log\log N)$ and $h \in \mathbf{Z}$, then

$$\left| |\{n : n \in W_D(N), n \equiv h (\operatorname{mod} m)\}| - \frac{1}{m} |W_D(N)| \right| < \frac{c_2}{m} |W_D(N)| \exp\left(-c_3 \frac{\log N}{\log m}\right).$$

Theorem 2 is sharp in the follwing sense: there exists $c_4(g)$ such that for $D = \{0, 1\}$ and sufficiently large N there exist m and h such that

$$m < \exp(c_4 \log N / \log\log N)$$

but

$$\left| |\{n : n \in W_D(N), n \equiv h (\operatorname{mod} m)\}| - \frac{1}{m} |W_D(N)| \right| > \frac{1}{m} |W_D(N)|.$$

I have not be able to prove or disprove that for $m < N^{c(g)}$, $(m, g) = 1$ the set $W_D(N)$ meets every residue class modulo m.

REFERENCES

[1] P. Erdös, C. Mauduit and A. Sárközy, On arithmetic properties of integers with missing digits. I: Distribution in residue classes, J. Number Theory **70** (1998), 99–120.

kon@nw.math.msu.su

Diophantine approximation by cubes of primes and an almost prime

Angel Koumtchev /Kumchev/
University of South Carolina

Let $a_1, \dots, a_k$ be real numbers with a_1/a_2 irrational and consider the form

$$a_1 x_1^3 + \dots + a_k x_k^3. \tag{1}$$

We will show that if $k = 4$ almost all real numbers can be "well approximated" by the values taken by (1) when $x_2, \dots, x_4$ are prime and x_1 is a P_6 (i.e. has at most 6 prime divisors). This will imply that in the case $k = 8$ the values attained by (1) when x_1 is a P_6 and the remaining variables are prime are dense in $\mathbf{R}$.

koumtche@math.sc.edu

Forty-eight irreducibility theorems (and still no thesis)

Robert F. Murphy
University of South Carolina

A polynomial $f(x)$ is said to be reciprocal if $f(x) = \pm x^{\deg f} f(1/x)$. The non-reciprocal part of $f(x)$ is $f(x)$ with its irreducible reciprocal factors removed. Selmer (1956) and Tverberg (1960) show that the non-reciprocal part of $f(x) = x^n \pm x^a \pm 1$ is irreducible (or ± 1). Ljunggren (1960) and Mills (1985) show that the non-reciprocal part of $f(x) = x^n \pm x^b \pm x^a \pm 1$ is irreducible (or ± 1) unless $f(x)$ takes on certain specified forms. Filaseta and Solan recently obtained results for five and six-term polynomials with each coefficient equal to $+1$. We discuss a general algorithm for obtaining such results and classify all five and six-term polynomials with coefficients equal to ± 1 whose non-reciprocal parts are reducible.

murphy@math.sc.edu

Integer points close to a smooth curve

Ognian Trifonov
University of South Carolina

Huxley and T. proved recently that the interval $(x, x+h]$ contains the "right" number of squarefull integers namely $\frac{\zeta(3/2)}{2\zeta(3)}x^{\theta}(1+o(1))$ when $h = x^{1/2+\theta}$, $\theta > 1/8$ and x is sufficiently large. To prove this result estimates for the number of integer points close to a certain smooth curve are needed. We improve on these estimates and as a result we extend the range of admissible values for θ below 1/8.

trifonov@math.sc.edu

Generalized Kummer Congruences

Paul T. Young
College of Charleston

Kummer's congruences for the Bernoulli numbers have been generalized and strengthened in many ways. In this paper we consider two of the strongest forms of these congruences, and begin with a general theorem on sequences which exhibit analogous congruences. We then demonstrate generalizations of Kummer congruences for values of Bernoulli polynomials and generalized Bernoulli polynomials. These values interpolate values of Hurwitz zeta functions and two-variable p-adic L-functions. We also give a general theorem on Kummer congruences for degenerate sequences.

paul@math.cofc.edu

Average size of 2-Selmer groups of a family of elliptic curves

Gang Yu
Department of Mathematics, The University of Georgia, Athens, GA 30605

Suppose X is a large positive real number. We show an asymptotic formula for the average size of 2-Selmer groups of elliptic curves given by the equation

$$y^2 = x(x+p)(x+q),$$

where $-X \le p \ne q \le X$ with both $|p|$ and $|q|$ being prime.

For curves given by the equation

$$y^2 = x(x+a)(x+b)$$

with a a fixed non-zero integer, we show that, when varying $b \in [-X, X]$, the average size of the 2-Selmer groups is unbounded if $|a|$ is a perfect square, and is bounded otherwise.

The results provide an approach to a conjecture of A. Brumer.

gyu@alpha.math.uga.edu