WORKSHOP
Pseudorandomness in Number Theory (1326)
Dates: 14-18 July 2014 at CIRM (Marseille, France)

SCHEDULE

Pseudorandomness in number theory
14–18 July 2014

Program

Tuesday 15/07

10:00–10:45	**Mariusz Lemanczyk**, *Intrinsic ergodicity of B-free systems*
10:45–11:15	Coffee Break
11:15–12:00	**Nikos Frantzikinakis**, *Gowers uniformity of multiplicative functions and applications*
14:30–16:00	**Problem Session**, *Forming small working groups*
16:00–16:30	Coffee Break
16:30–19:30	*Work in small groups*

Wednesday 16/07

10:00–10:45	**Cécile Dartyge** , *On the greatest prime factor of a polynomial of degree four*
10:45–11:15	Coffee Break
11:15–12:00	**TBA**,
14:30–15:15	**Domingo Gómez-Pérez**, *On the linear complexity and lattice test of nonlinear pseudorandom number generators*
15:20–16:05	**Min Sha**, *A preferable linear recurrence sequence can be generated randomly*
16:05–16:30	Coffee Break
16:30–19:30	*Work in small groups*

Thursday 17/07

10:00–10:45	**John Boxall**, *Heuristics on pairing-friendly elliptic curves and abelian varieties*
10:45–11:15	Coffee Break
11:15–12:00	**Claus Diem**, *Remarks on linear complexity*
14:30–15:15	**TBA**,
15:20–16:05	**TBA**,
16:05–16:30	Coffee Break
16:30–19:30	*Work in small groups*

Friday

10:00–12:30	*Work in small groups*