Name Makoto Matsumoto
Research Area Number Theory, Applied Mathematics
Keywords Arithmetic Fundamental Groups, Pseudorandom Number Generation
Current Researches My research subjects are:

(a) Via arithmetic fundamental groups, study interactions between number theory and topology.

(b) Using algebraic/geometric algorithms, design and deliver practical algorithms such as pseudorandom number generators.

(a) In topology, a geometric object X is studied through its algebraic invariants, such as its cohomology groups and the fundamental group. For an algebraic variety X, there is a notion of the etale cohomology and the etale fundamental group. When the variety is defined over a field K, the absolute Galois group G_K acts on these algebraic invariants. If K is a subfield of the complex number field and the embedding $\overline{K} \subset \mathbb{C}$ is fixed, then the etale fundamental group of $X \otimes \overline{K}$ is canonically isomorphic to the profinite completion (a mechanical operation on abstract groups) of the ordinal fundamental group of X, regarded as a complex manifold.

A number-theoretic important group G_K (depending only on K) and the etale fundamental group of $X \otimes \overline{K}$ (depending only on the homotopy type of X) are intertwined via this action. For famous X such as curves and moduli spaces of curves, the usual fundamental group of X is well studied and deep results are obtained by topologists. Using them, I obtain number-theoretic results which might be hard to prove without topological results. Conversely, number theoretic results sometimes imply non-trivial fact in topology.

Most mathematicians in arithmetic geometry might have more interest in cohomology theory, but I am interested in fundamental groups because they have more information (due to its non-abelian property), and results of low dimensional topologies (such as mapping class groups) can be effectively used.

(b):"With a great precision, generate a sequence of numbers which mimics a random sequence." This requirement appears in any computer simulation including some random events. Answers to this requirement are called "pseudorandom number generators." Unexpectedly, linear algebra over finite field does good job in this area. Many good pseudorandom number generators are based on linear recursion over the two-element field. To assure the period, one needs to obtain its characteristic polynomials (say, by Berlekamp-Massey method). To analyze high-dimensional equidistributedness, we use algebraic and geometric algorithms based on the lattice reduction. Here the lattice means a discrete $\mathbf{F}_2[t]$-module in $\mathbf{F}_2((t^{-1}))^N$. We study algorithms which are appropriate to the recent architecture of CPU (including Graphic Processing Units), using mathematics. An interesting and important problem is how to evaluate the generators. There are many subjects to attack.

Prerequisits to Students In arithmetic geometry, very wide and deep notions in mathematics are used, and I myself feel much difficulty to cover them. Students need to spend enough time to learn the fundamental materials, such as schemes, site, etc. When I digest abstract notions and understand what they really mean, I feel a deepest pleasure in life.

As for pseudorandom number generation, it is easier to start to study. However, when you try to invent something which is really practical, you need to work hard and widely. For example, you need to write a code, to experiment, to think what is the missing information for the success (it might be the architecture of CPU, statistics, how random numbers are actually used, combinatorial design, Riemann-Roch, Fourier transform, or anything). All these processes are hard, but will become a great pleasure when they work out.