On the Randomness of Modular Inverse Mappings

Jonathan Bober

February 6, 2003

Abstract

In this paper the randomness of the inverse mapping of a finite field is investigated in the context of random permutations. The function $x \to x^{-1} \mod p$, p a prime, is studied as a permutation of the integers from 1 to $p-1$. Specifically, the function is its own inverse and is signed, so it forms a signed involution. Baik, Deift, and Johansson [1] and Baik and Rains [3] have given results concerning the distribution length of the longest increasing subsequence of a random permutation and of certain subsets of random permutations (such as a signed involution). These distributions are either the same as or are expressed in terms of the Tracy-Widom distributions for the largest eigenvalue of a random matrix from certain matrix ensembles. Calculations suggest that the same is true of the permutations from the inverse mapping, and, specifically, it is conjectured that, looked at in the right way, the distribution of the length of the longest increasing subsequence of the inverse mapping is asymptotically the same as the case of a random fixed point free signed involution.

1 Introduction

Arithmetic of integers modulo a prime forms the finite field $\mathbb{Z}/p\mathbb{Z}$. In this field the question arises of whether certain arithmetic operations exhibit properties of "randomness".

Evidence already exists for some "randomness" of this function. The Hooley R^* conjecture surmises that the partial Kloosterman sum

$$\left| \sum_{A \leq x \leq A+N} e\left(\frac{cx^{-1}}{p}\right) \right| \ll N^{1/2} p^{\epsilon}, \epsilon > 0$$

where $e(x) = e^{2\pi i x}$ and $i = \sqrt{-1}$.

This is known true for $N > \sqrt{p}$, by Weil's bound on Kloosterman sums [5]. Of course, the full sum

$$|Kl\,(0,1,p))| = \left| \sum_{1 \leq x < p} e\left(\frac{x^{-1}}{p}\right) \right| = \left| \sum_{1 \leq x < p} e\left(\frac{x}{p}\right) \right| = 1,$$

because it is the sum of the p pth-roots of 1, excluding the root 1. Intuitively, if $x \rightarrow x^{-1}$ is a random mapping, then this sum should take on small values over a large enough interval, as is partially known. Though it is not the focus of this paper, it would be instructive and interesting to test Hooley's conjecture to examine whether it may hold up.

Another way in which this "randomness" can be investigated is through permutations. The mapping $x \rightarrow x^{-1}$ is one-to-one on the set $\mathbb{Z}/p\mathbb{Z} - \{0\}$ and the ordering $1^{-1}, 2^{-1}, ..., (p-1)^{-1}$ defines a permutation of the set $1...(p-1)$. This permutation is an almost fixed point free signed involution.

Definition 1 (Involution). *A permutation $\pi(x)$ is an involution if it is the product of disjoint 2-cycles, or equivalently, if $\pi(\pi(x)) = x$.*

Definition 2 (Signed permutation). *A permutation $\pi_n(x)$ of $n-1$ elements is signed if $P(-x) = -P(x)$, where the arithmetic inverse is defined as normal in the ring $\mathbb{Z}/n\mathbb{Z}$, where $x + (-x) = 0 \mod n$.*

Definition 3 (Fixed and negated points). *A fixed point in a permutation $\pi(x)$is an x for which $\pi(x) = x$. A negated point is an x for which $\pi(x) = -x$.*

The permutation on the set $\{1, 2, 3, 4, ..., p-1\}$ defined by $x \rightarrow x^{-1} \mod p$, p prime, is a signed involution because $(x^{-1})^{-1} = x$ and $(-x)^{-1} = -x^{-1}$. It is almost fixed point free because the equation $x^2 = 1$ can have at most 2 solutions in $\mathbb{Z}/p\mathbb{Z}$, and it has the two solutions ± 1. The two fixed points will have no effect on the asymptotic statistics of these permutations.

2 Random permutations and the Tracy-Widom distributions

Let π be a random permutation of n elements. We say that $\pi(i_1), \pi(i_2), ...\pi(i_k)$ is an increasing subsequence of π with length k if $\pi(i_1) < \pi(i_2) < ... < \pi(i_k)$ and $i_1 < i_2 < ... < i_k$. For example, if π maps 1 2 3 4 5 6 7 to 3 5 1 6 7 2 4, than the longest increasing subsequence of π is 3 5 6 7, with length 4.

The asymptotics of the distribution of the length of the longest increasing subsequence for a random permutation have been much computed and studied and have been fully solved by Baik, Deift and Johanson in [1]. Also, Baik and Rains have solved the asymptotics for various types of permutations [3]. Some of these results are restated below.

2.1 Tracy-Widom distribution functions

Let $u(x)$ be the solution to the Painleve II equation

$$u_{xx} = 2u^3 + xu,$$

with the condition that $u(x) \to -Ai(x)$ as $x \to +\infty$, where $Ai(x)$ is the Airy function. The existence and uniqueness of the function is established in [4]. Define

$$v(x) := \int_{\infty}^{x} (u(s))^2 ds$$

.

Definition 4 (Tracy-Widom Distribution). *Define*

$$\begin{array}{rcl} F(x) & := & exp\left(\frac{1}{2}\right) \int_x^\infty v(s)ds, \\ E(x) & := & exp\left(\frac{1}{2}\right) \int_x^\infty u(s)ds, \end{array}$$

and then set

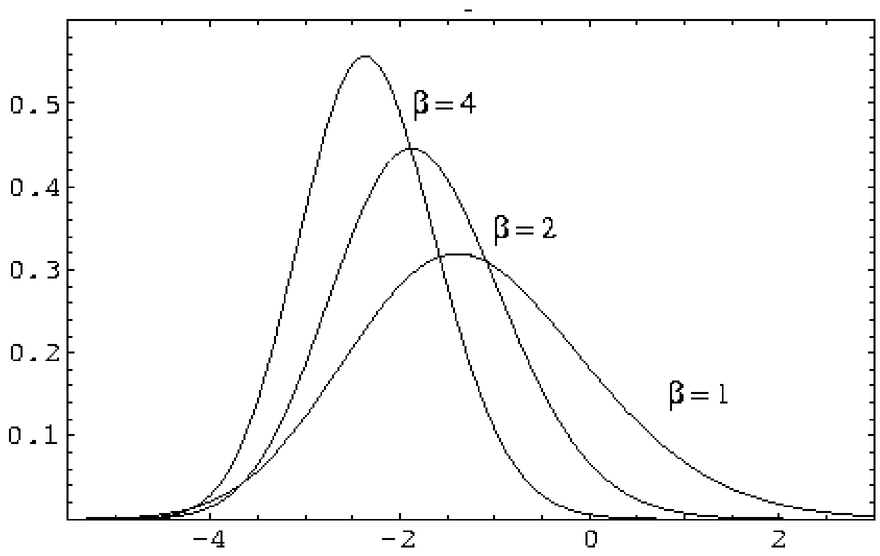
$$\begin{array}{rcl} F_2(x) & := & F(x)^2, \\ F_1(x) & := & F(x)E(x), \\ F_4(x) & := & F(x)[E(x)^{-1} + E(x)]/2 \end{array}$$

It is interesting to note that these distributions are not centered around 0. Each of them has negative mean. In both the random matrix model and random permutation model, these distributions arise in the exploration of deviation around an asymptotic mean. In both cases, however, the asymptotic mean used for the distribution is just a first order approximation, and the true asymptotic mean is fully solved. Once the true mean is obtained, it seems that it would make more sense to center the distributions around this mean, but this was not done, and thus these distributions are off center.

Tracy and Widom have shown that $F_1(x), F_2(x)$ and $F_4(x)$ are the asymptotic distribution functions for largest eigenvalues of the Gaussian matrix ensembles for $\beta = 1, 2, 4$ (suitably rescaled.) Moreover, in [1] Baik, Deift and Johanson showed that for a random permutation, the distribution of

$$\frac{L_n - 2\sqrt{n}}{n^{\frac{1}{6}}}$$

Figure 1: Tracy-Widom distribution functions



also converges to $F_2(x)$. In [3], Baik and Rains give results for various types of random permutations, all of which are also related to the three Tracy-Widom distribution functions.

2.2 Random Permutations

Let S_n be the set of all permutations of n elements, and define $fp(P)$ the number of fixed points of the permutation $P(x)$ and $np(P)$ the number of negated points. Define:

$$\begin{aligned}
S_n^{\square} &= S_n \\
S_{n,m}^{\boxslash} &= \{P(x) \in S_{2n+m} : P(P(x)) = x, fp(P) = m\} \\
S_{n,m}^{\boxbslash} &= \{P(x) \in S_{2n+m} : P(x) = -P^{-1}(x), np(P) = m\} \\
S_n^{\boxdot} &= \{P(x) \in S_{2n} : P(-x) = -P(x)\} \\
S_{n,m_+,m_-}^{\boxtimes} &= \{P(x) \in S_{4n+2m_++2m_-} : P(-x) = -P(x), P(P(x)) = x, \\
&\quad\; fp(P) = 2m_+, np(P) = 2m_-\}
\end{aligned}$$

and the random variables

$$L_n^{\square}, L_{n,m}^{\boxslash}, L_{n,m}^{\boxbslash}, L_n^{\boxdot}, L_{n,m_+,m_-}^{\boxtimes}$$

as the length of the longest increasing subsequence of a random permutation chosen uniformly from the corresponding set above.

In language closer to english, $S^{\boxslash}_{n,m}$ is the set of involutions of $2n+m$ elements with m fixed points, $S^{\boxdot}_{n}$ is the set of signed permutations of $2n$ elements, and $S^{\boxtimes}_{n,m_+,m_-}$ is the set of signed involutions of $4n+2m_+ +2m_-$ elemtents with $2m_+$ fixed points and $2m_-$ negated points. If the notation seems a bit odd, it is because it is a bit odd, but it is taken from the context of [3], in which it makes more sense.

For each of the random variables, $L^{\circledast}$ with $m, n \leq \sqrt{N}$ we have

$$\lim_{N\to\infty} \frac{E(L^{\circledast})}{\sqrt{N}} = 2$$

and for each we have an asymptotic distribution, with fixed x, α, β

$$\begin{array}{lcl}
\lim_{n\to\infty} \Pr\left(\frac{L^{\square}_{n}-2\sqrt{N}}{N^{1/6}} \leq x\right) & = & F_2(x), \\
\lim_{n\to\infty} \Pr\left(\frac{L^{\boxdot}_{n,m}-2\sqrt{N}}{2^{2/3}N^{1/6}} \leq x\right) & = & F_2(x)^2, \\
\lim_{n\to\infty} \Pr\left(\frac{L^{\boxslash}_{n,[\sqrt{2n}\alpha]}-2\sqrt{N}}{N^{1/6}} \leq x\right) & = & \left\{\begin{array}{rll} F_4(x) & \text{if} & 0 \leq \alpha < 1; \\ F_1(x) & \text{if} & \alpha = 1; \\ 0 & \text{if} & \alpha > 1. \end{array}\right. \\
\lim_{n\to\infty} \Pr\left(\frac{L^{\boxbslash}_{n,[\sqrt{2n}\beta]}-2\sqrt{N}}{N^{1/6}} \leq x\right) & = & F_1(x), \beta \geq 0, \\
\lim_{n\to\infty} \Pr\left(\frac{L^{\boxtimes}_{n,[\sqrt{n}\alpha],[\sqrt{n}\beta]}-2\sqrt{N}}{2^{2/3}N^{1/6}} \leq x\right) & = & \left\{\begin{array}{rll} F_2(x) & \text{if} & 0 \leq \alpha < 1, \beta \geq 0; \\ F_1(x)^2 & \text{if} & \alpha = 1, \beta \geq 0; \\ 0 & \text{if} & \alpha > 1, \beta \geq 0. \end{array}\right.
\end{array}$$

2.3 Relation to Modular Inverse Mapping

Because these distributions arise in the context of random permutations, we investigate whether they might arise in the permutation defined by $x \to x^{-1}$. Specifically, because $x \to x^{-1}$ defines a fixed point free involution, we investigate whether the asymptotic distribution of the longest increasing subsequence of the involution is the function $F_2(x)$, and whether the distribution scales the same way as for a fixed point free involution.

Let L_p be the length of the longest increasing subsequence of the permutation $\pi_p(x)$ defined by $x \to x^{-1} \mod p$, and define

$$S_{N,K} = \{L_p(x) : N - K(\log(N))^{1+\epsilon} \leq p \leq N + K(log(N))^{1+\epsilon}\}$$

for $\epsilon = 1$ or 2, for example. Note that N need not be prime in this definition.

By the Prime Number Theorem, this set has approximately $(log(N))^{\epsilon}$ elements, and thus as $N \to \infty$, $|S_{N,K}| \to \infty$. Additionally, we have, for fixed

K

$$\lim_{N\to\infty} \frac{K(log(N))^{1+\epsilon}}{\sqrt{N}} = 0$$

so that, if the mean is asymptotic to $2\sqrt{N}$ then, in this set, L_p will not change too much, and also, if the permutation behaves randomly will see that the mean of each set, $\mu(N)$ (just one function for the mean is defined, as it will change very little for reasonable intervals, and not at all in the limit as $N \to \infty$) will be asymptotic to $2\sqrt{N}$

Additionally, we look at the standard deviation of each set around an N. Define

$$\sigma(N) = \sqrt{\frac{1}{|S_{N,K}|} \sum_{L(p)\in S_{N,K}} (L_p - \mu(p))^2}$$

and now we hope to see that $\sigma(N)$ is aymptotic to $2^{2/3}N^{1/6}$.

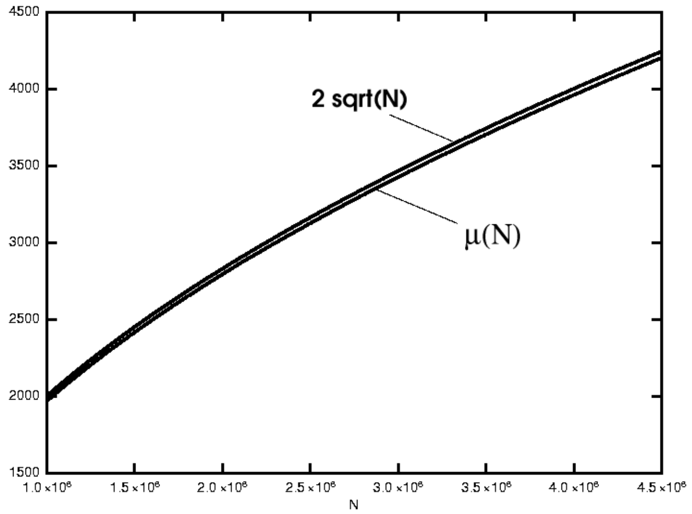
Also, various comparisons are made between computed distributions and asymptotic distributions.

3 Computations and Results

3.1 Mean and Deviation

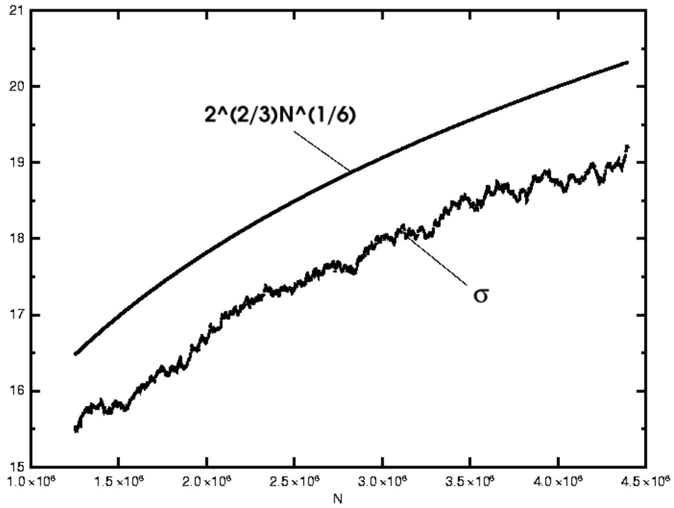
For $\epsilon = 1, K = 1000$, we have the following for $\mu(N)$, from 1000000 to 4500000

Figure 2: $2N^{1/2}$ and $\mu(N)$



$\mu(N)$ remains just below $2\sqrt{N}$ over the entire interval, suggesting that it is asymptotic to $2\sqrt{N}$, and it indeed appears to be $O(N^{1/6})$ away from $2\sqrt{N}$, as is shown by looking at the deviation compared to $2^{2/3}N^{1/6}$.

Figure 3: Standard Deviation



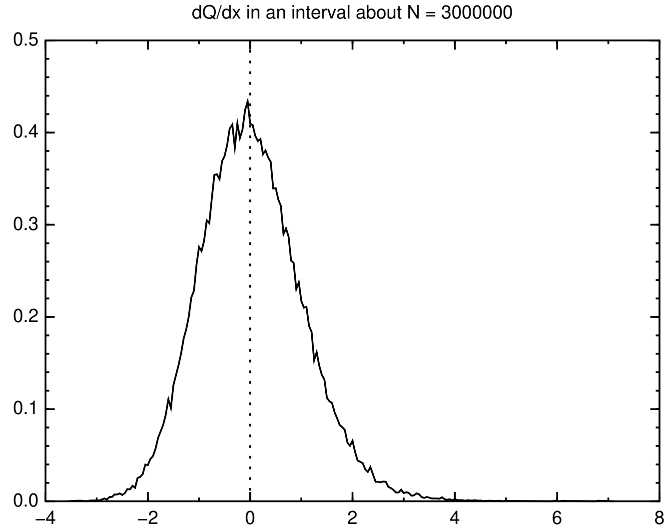
Both the mean and the standard deviation seem to be well within what would be expected for random involutions.

3.2 Comparisons to Random Permutations

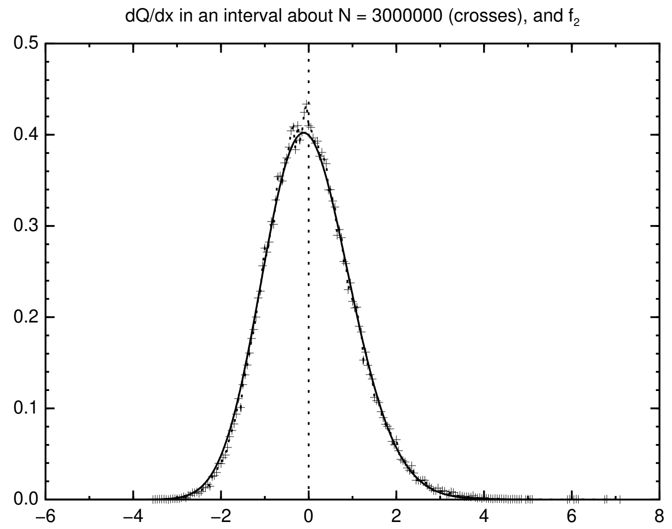
Now for an even larger interval we examine the random variable we examine the set $\hat{S}_N = \{\chi(p) = L_p - \mu(p)\}$ for p in an interval about N. After obtaining the standard deviation of this set, we examine the function

$$Q_N(x) = \Pr\left(\frac{\chi(p)}{\sigma(S_N)} \leq x\right)$$

and differentiate to obtain the normalized probability density function $\frac{dQ_N}{dx}$ with mean 0 and standard deviation 1.

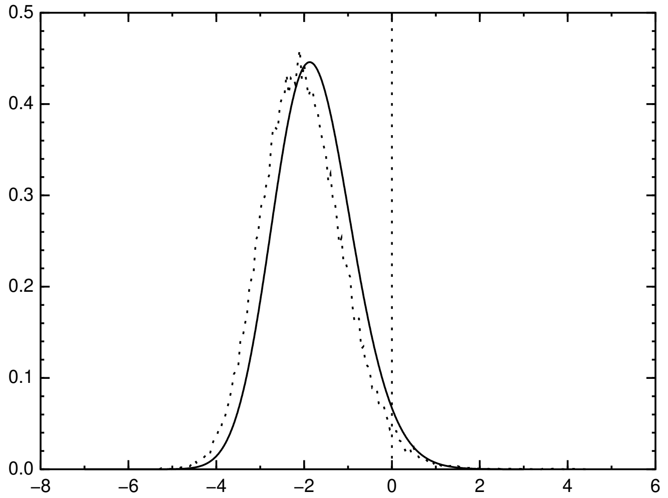


Compared to the normalized derivative of the Tracy-Widom distribution function $F_2(x)$, a possible relation is seen.



Of course, this visual itself is not too strong of evidence that the two functions are the same asymptotically. In fact, when normalized to have mean 0 and standard deviation 1, all three Tracy-Widom distribution functions are virtually inditinguishable to the eye. It is the normalization factors above that provide stronger evidence of correlation, and thus it is instructive

Figure 4: $f_2(x)$ and $d\hat{Q}_N(x)/dx$(dotted)



to look at the function

$$\hat{Q}_N(x) = \Pr\left(\frac{L_p - 2\sqrt{p}}{2^{2/3}p^{1/6}} \leq x\right), L_p \in S_{N,K}$$

in an interval around N as compared to $F_2(x)$ as defined originally.

Figure 4 shows a graph for $N = 3000000$ and a rather large interval. The graph of $f_2(x)$ is a bit to the right of the computed graph. This result shows what was shown in part in both the mean and standard deviation plots above, and a bit more. First, the mean is significantly less than $2\sqrt{N}$, though asymptotically similar, and, moreso, is less than the mean of the Tracy-Widom function. Second, the standard deviation is significantly less than $2^{2/3}p^{1/6}$, though again asymptotically similar. The fully normalized graph is a more natural graph to make, as the mean and the deviation about that mean are separate issues, but there is still something instructive in the graphs that do not have mean 0, and they allow more in the way of visual comparison.

We have the following statistics of the probablity density function $d\hat{Q}_N(x)/dx$ for intervals $[a, b]$:

a	b	Mean	Variance	Std Dev
0	1000000	-2.02129	.860861	.927826
1000000	2000000	-2.04177	.871930	.933772
2000000	3000000	-2.03890	.884904	.940694
3000000	4000000	-2.04323	.887816	.942240
4000000	5000000	-2.04980	.873988	.934873
All computed values		-2.03687	.876913	.936436
Possible aysmptotic expectation		-1.77109	.813189	.901770

4 Conclusions and the Future

This data is by no means fully conclusive, and without theoretical conclusions, more computed data is necessary to obtain a better understanding of this problem. However, it seems safe to make the following conjectures:

Conjecture 1.

$$\lim_{N\to\infty} \frac{\mu(N)}{\sqrt{N}} = 2$$

and (slightly less safe)

Conjecture 2.

$$\lim_{N\to\infty} \frac{\sigma(N)}{N^{1/6}} = 2^{2/3}$$

which are the same as the values of the limits for a random fixed point free signed involution.

Also, it seems plausible that

$$\lim_{N\to\infty} \hat{Q}_N(x) = F_2(x)$$

but it seems that current data is not nearly enough to conjucture on whether this statement is true or false. Current data suggests that this is not true, but that a rescaling by simply subtracting a value other than $2\sqrt{N}$ may make the statement true. In truth, I am not willing to make a guess either way, but will guess that these permutations are indeed related to random permutations somehow.

In order to make a better comparison between inverse mapping permutations and random permutations, it might be good to look at the length of the longest increasing subsequence after the first is removed, and then remove that and continue. This is equivalent to building what are called Young tableaux, which for random permutations are also related to the eigenvalues for random matrices [2].

Also, while asymptotics are known for fixed point free involutions, there is not much numerical data to compare to. It is possible, though probably not likely, that convergence to the Tracy-Widom distribution requires very long permutations and numerical data may show that in the range that has been computed for the inverse mappings, they actually do behave exactly like a random involution.

Other tests can also shine light on the randomness of this mapping. Hooley's conjecture should be numerically tested, and also, the distribution of $x \to x^{-1}$, with fixed p can be investigated for a range of x less than p to test for randomness in distribution and for correlation in spacings. Moreover, one can look at the distribution of the inverse of a fixed x for varying primes. Very simple tests on both of these that I did seemed to suggest randomness, but the tests were extremely simple, and while they do not debunk any theories of randomness, neither do they provide evidence.

If anyone continues any of these calculations, please contact me (jwb235@nyu.edu or bober@acm.cs.nyu.edu,) as it is quite possible that I will have more data available in the future.

5 Computational methods

The algorithms used were mostly rather standard and simple, and all code for computation was written in C++. The NTL (see http://www.shoup.net) was used for its library functions and occasionally for multiprecision arithmetic. Full source code should hopefully be available from whatever website you retrieved this paper from (if you did so.) It will also be available at http://www.math.nyu.edu/Courses/V63.0393/ and http://acm.cs.nyu.edu/ bober/math/ and will hopefully be well documented and commented, so that it may be used and modified by anyone who wishes to do so.

Note: The algorithm used to computer the longest increasing subsequence is not bad but and can be improved upon with a more complicated method.

In the next few weeks I hope to program a better algorithm that will be faster and will also compute all increasing subsequences.

6 Acknowledgements

Looking at the longest increasing subsequence of these permutations was first suggested to Steven Miller and Peter Sarnak by Jim Propp, who suggested that such conjectures as made above could probably be made.

Also, much thanks goes to Professor Sarnak, Steve Miller and Alex Barnett, for running a class with as many instructors as students, and to Brad Weir and Tim Novikoff, without whom the class probably would not have existed in such a form. Discussions with all were extremely useful. And also thanks to Craig Tracy for providing Mathematica code for the Tracy-Widom distribution functions.

7 References

[1] J. Baik, P. Deift, and K. Johansson. On the distribution of the length of the longest increasing subsequence of random permutations. *J. Amer. Math. Soc.*, 12:1119-1178,1999 and e-print math.CO/9810105

[2]J. Baik, P. Deift, and K. Johansson. On the distribution of the length of the second row of a Young diagram under Plancherel measure. e-print math.CO/9901118

[3]J.Baik and E. M. Rains. Symmetrized random permutations. e-print math.CO/9910019

[4]S. P. Hastings and J. B. McLeod, A boundary value problem associated with the second Painleve transcendent and the Korteweg de Vries equation, *Arch. Rational Mech. Anal.* 73,31-51, (1980)

[5]D.R. Heath-Brown. "Arithmetic applications of Kloosterman sums", September 2000