Biases in the Shanks–Rényi Prime Number Race

Greg Martin
University of British Columbia

Foundations of Computational Mathematics
Workshop on Computational Number Theory

Institute for Mathematics and its Applications
University of Minnesota, Minneapolis
August 8, 2002

Primes in arithmetic progressions

The main object of study is

$$\pi(x;q,a) = \#\{\text{primes } p \le x \colon p \equiv a \pmod{q}\}$$

Dirichlet proved in 1837 that as long as $\gcd(q,a) = 1$, there are *infinitely many primes congruent to* $a \pmod{q}$.

Chebyshev remarked in 1853 that there seem to be more primes congruent to $3 \pmod 4$ than to $1 \pmod 4$.

Similar *biases* have been observed to other moduli, notably by Shanks in 1959.

$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
5	3
13	7
17	11
29	19
37	23
41	31
53	43
61	47
73	59
89	67
97	71
101	79
109	83
113	103
137	107
149	127
157	131
173	139
181	151
193	163

$p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$
7	2
13	5
19	11
31	17
37	23
43	29
61	41
67	47
73	53
79	59
97	71
103	83
109	89
127	101
139	107
151	113
157	131
163	137
181	149
193	167

$p \equiv 1 \pmod 5$ $p \equiv 3 \pmod 5$

$p \equiv 2 \pmod 5$ $p \equiv 4 \pmod 5$

11	2	3	19
31	7	13	29
41	17	23	59
61	37	43	79
71	47	53	89
101	67	73	109
131	97	83	139
151	107	103	149
181	127	113	179
191	137	163	199
211	157	173	229
241	167	193	239
251	197	223	269
271	227	233	349
281	257	263	359
311	277	283	379
331	307	293	389
401	317	313	409
421	337	353	419
431	347	373	439

Classical analytic results

It was proved in the 1890s, independently by Hadamard and de la Vallée Poussin (with contributions from von Mangoldt, and all based on Riemann's 1860 memoir), that

$$\pi(x;q,a) \sim \frac{\mathrm{li}(x)}{\phi(q)}$$

when $\gcd(q,a)=1$, where

$$\mathrm{li}(x) = \int_2^x \frac{dt}{t} \sim \frac{x}{\log x}.$$

In particular,

$$\lim_{x\to\infty} \frac{\pi(x;q,a)}{\pi(x;q,b)} = 1$$

when $\gcd(q,a)=\gcd(q,b)=1$.

However, the biases exist because the analytic objects in the proofs "naturally" count prime powers (in particular, *squares of primes*).

For example, for $\operatorname{Re} s > 1$ the *Riemann zeta-function* is given by

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{\text{primes } p} (1 - p^{-s})^{-1}$$

and so

$$\begin{aligned}
\log \zeta(s) &= \sum_{\text{primes } p} \log(1 - p^{-s})^{-1} \\
&= \sum_{\text{primes } p} \sum_{k=1}^{\infty} \tfrac{1}{k} p^{-ks} \\
&= 2^{-s} + 3^{-s} + \tfrac{1}{2} 4^{-s} + 5^{-s} + 7^{-s} + \tfrac{1}{3} 8^{-s} \\
&\qquad + \tfrac{1}{2} 9^{-s} + 11^{-s} + 13^{-s} + \tfrac{1}{4} 16^{-s} + \dots .
\end{aligned}$$

Similarly, related to primes in arithmetic progressions modulo q are the *Dirichlet L-functions*, given for $\operatorname{Re} s > 1$ by

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_{\text{primes } p} (1 - \chi(p) p^{-s})^{-1},$$

where χ is a *Dirichlet character* $\pmod q$, that is, a function on the integers with period q satisfying

$$\chi(mn) = \chi(m)\chi(n)$$

and

$$\chi(n) \neq 0 \iff \gcd(q,n) = 1.$$

$p^k \equiv 1 \pmod 4$	$p^k \equiv 3 \pmod 4$	$p^k \equiv 1 \pmod 3$	$p^k \equiv 2 \pmod 3$
5	3	4	2
9	7	7	5
13	11	13	8
17	19	16	11
25	23	19	17
29	27	25	23
37	31	31	29
41	43	37	32
49	47	43	41
53	59	49	47
61	67	61	53
73	71	64	59
81	79	67	71
89	83	73	83
97	103	79	89
101	107	97	101
109	127	103	107
113	131	109	113
121	139	121	125
125	151	127	128
137		139	131
149		151	137
157		157	

Comparing the functions $\pi(x;q,a)$ to each other

It was a surprise when Littlewood proved in 1914 that both $\pi(x;4,3) - \pi(x;4,1)$ and $\pi(x;3,2) - \pi(x;3,1)$ changed sign infinitely often.

Other results about sign changes of $\pi(x;q,a) - \pi(x;q,b)$ were established, mostly subject to hypotheses on the location of zeros of Dirichlet L-functions, by Knapowski and Turán in the 1960s and by Kaczorowski in the 1990s.

$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
26717	26683
26729	26687
26737	26699
26777	26711
26801	26723
26813	26731
26821	26759
26833	26783
26849	26839
26861	26863
26881	26879
26893	26891
26921	26903
26953	26927
26981	26947
26993	26951
27017	26959
27061	26987
27073	27011
27077	27031

$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
616673	616547
616717	616579
616729	616639
616741	616643
616757	616703
616769	616723
616789	616783
616793	616787
616829	616799
616841	616843
616849	616871
616877	616943
616897	616951
616909	616991
616933	616999
616961	617011
616997	617027
617053	617039
617077	617051
617129	617059

$$\pi(26{,}861; 4, 1) = 1{,}473 = \pi(26{,}861; 4, 3) + 1$$

$$\pi(616{,}841; 4, 1) = 25{,}189 = \pi(616{,}841; 4, 3) + 1$$

(Leech 1957)

$p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$
608981812531	608981811929
608981812651	608981812037
608981812717	608981812391
608981812759	608981812613
608981812771	608981812667
608981812867	608981812697
608981812891	608981812709
608981812951	608981812721
608981812993	608981812919
608981813017	608981812961
608981813029	608981813123
608981813137	608981813261
608981813191	608981813273
608981813269	608981813303
608981813311	608981813357
608981813347	608981813459
608981813449	608981813501
608981813569	608981813507
608981813677	608981813621
608981813683	608981813711

$$\pi(608{,}981{,}813{,}029; 3, 1) = 11{,}669{,}295{,}396 = \pi(608{,}981{,}813{,}029; 3, 2) + 1$$

(Bays and Hudson 1978)

The work of Rubinstein and Sarnak

In 1994, Rubinstein and Sarnak proved some striking results under the following two hypotheses:

GRH (the Generalized Riemann Hypothesis): all zeros of Dirichlet L-functions in the critical strip $0 < \operatorname{Re} s < 1$ actually lie on the line $\operatorname{Re} s = \frac{1}{2}$

LI: the nonnegative imaginary parts of these zeros are all Linearly Independent over the rational numbers

Define a "density"

$$\delta_{q;a_1,\dots,a_r} = \lim_{x\to\infty} \frac{1}{\log x} \int_2^x f_{q;a_1,\dots,a_r}(t) \frac{dt}{t},$$

where

$$f_{q;a_1,\dots,a_r}(t) = \begin{cases} 1, & \text{if } \pi(x;q,a_1) > \cdots > \pi(x;q,a_r), \\ 0, & \text{otherwise.} \end{cases}$$

Assuming GRH, $\delta_{q;a_1,\dots,a_r}$ exists.

Assuming GRH & LI, $\delta_{q;a_1,\dots,a_r} > 0$.

Moreover, if S, S' are squares modulo q and N, N' are nonsquares, then

$$0 < \delta_{q;S,N} < \tfrac{1}{2} < \delta_{q;N,S} < 1$$

and

$$\delta_{q;S,S'} = \tfrac{1}{2} = \delta_{q;N,N'}.$$

For example, $\delta_{4;3,1} \approx .9959$ and $\delta_{3;2,1} \approx .9990$.

Extending their ideas

In 2000, Feuerverger and M. extended the ideas of Rubinstein and Sarnak and made further calculations (under the same hypotheses GRH & LI).

For example, 1 and 4 are squares (mod 5) while 2 and 3 are nonsquares, and we calculated that

$$\delta_{5;2,1} = \delta_{5;2,4} = \delta_{5;3,1} = \delta_{5;3,4} \approx .9521$$

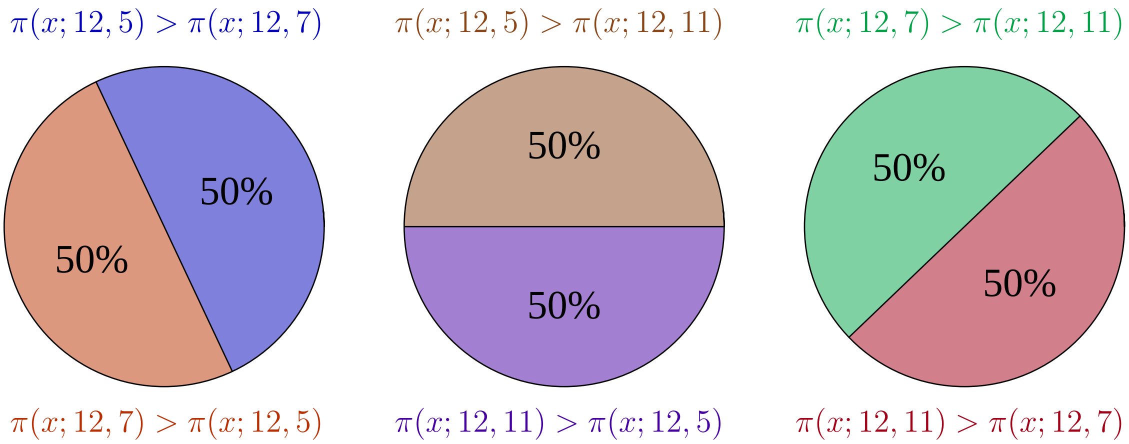
In contrast, 3, 5, and 7 are nonsquares (mod 8) while 1 is the only square; similarly, 5, 7, and 11 are nonsquares (mod 12) while 1 is the only square. We calculated that

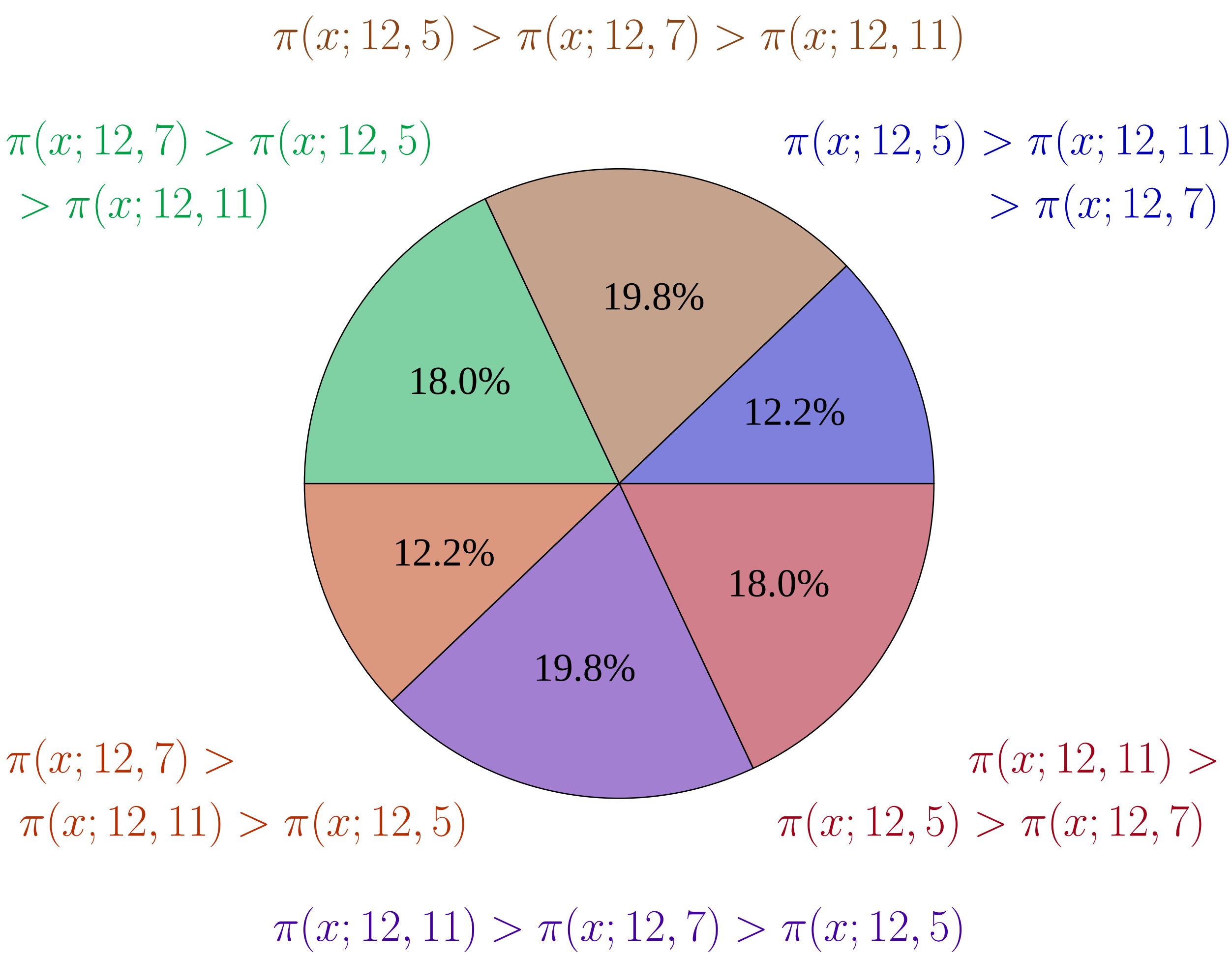
$$\delta_{8;3,1} \approx .99957 \qquad \delta_{12;5,1} \approx .99921$$

$$\delta_{8;5,1} \approx .99739 \qquad \delta_{12;7,1} \approx .99861$$

$$\delta_{8;7,1} \approx .99894 \qquad \delta_{12;11,1} \approx .99998$$

Regarding the three-way race among 5, 7, and 11 (mod 12):


$\pi(x;12,5) > \pi(x;12,7)$
$\pi(x;12,5) > \pi(x;12,11)$
$\pi(x;12,7) > \pi(x;12,11)$
50%
50%
50%
50%
50%
50%
$\pi(x;12,7) > \pi(x;12,5)$
$\pi(x;12,11) > \pi(x;12,5)$
$\pi(x;12,11) > \pi(x;12,7)$


$\pi(x;12,5) > \pi(x;12,7) > \pi(x;12,11)$
$\pi(x;12,7) > \pi(x;12,5) > \pi(x;12,11)$
$\pi(x;12,5) > \pi(x;12,11) > \pi(x;12,7)$
19.8%
18.0%
12.2%
12.2%
18.0%
19.8%
$\pi(x;12,7) > \pi(x;12,11) > \pi(x;12,5)$
$\pi(x;12,11) > \pi(x;12,5) > \pi(x;12,7)$
$\pi(x;12,11) > \pi(x;12,7) > \pi(x;12,5)$

Computation of $\delta_{12;5,7,11}$

Define a function $\mathbf{v} : \mathbb{R} \to \mathbb{R}^2$ by

$$\mathbf{v}(t) = 4te^{-t/2}\big(\pi(e^t;12,5) - \pi(e^t;12,7), \pi(e^t;12,7) - \pi(e^t;12,11)\big).$$

Notice that

$$\pi(e^t;12,5) > \pi(e^t;12,7) > \pi(e^t;12,11) \iff \mathbf{v}(t) \in \mathbb{R}^2_{>0}.$$

Rubinstein and Sarnak proved (on GRH & LI) that $\mathbf{v}(t)$ has a *limiting distribution function* $g(x,y)$ and that

$$\delta_{12;5,7,11} = \int_0^\infty \int_0^\infty g(x,y)\, dx\, dy.$$

Moreover, we have a formula for the Fourier transform $\hat{g}(x,y)$ (next slide).

Some almost standard analysis yields

$$\delta_{12;5,7,11} = \frac{1}{4} - \frac{1}{4\pi^2}\,\mathrm{PV} \iint_{\mathbb{R}^2} \frac{\hat{g}(x,y)}{xy}\, dx\, dy$$

(where PV denotes the Cauchy principal value).

What is $\hat{g}(x, y)$?

The function g can be interpreted as the distribution function for a sum of independent random variables; its Fourier transform can then be computed.

Recall the *Bessel function* $J_0(z) = \sum_{m=1}^{\infty} \frac{(-1)^m (z/2)^{2m}}{(m!)^2}$.

There are three nontrivial characters modulo 12: χ_{-3}, χ_{-4}, and χ_{12} (where $\chi_D(n) = \left(\frac{D}{n}\right)$).

If we define

$$F(z, \chi_D) = \prod_{\substack{\gamma > 0 \\ L(\frac{1}{2} + i\gamma, \chi_D) = 0}} J_0\left(\frac{2z}{\sqrt{1/4 + \gamma^2}}\right),$$

then we have the formula

$$\hat{g}(x, y) = F(2x, \chi_{-4}) F(2y - 2x, \chi_{-3}) F(-2y, \chi_{12}).$$

Obstacles to computing $\delta_{12;5,7,11}$

Recall that

$$\delta_{12;5,7,11} = \frac{1}{4} - \frac{1}{4\pi^2}\,\mathrm{PV}\iint_{\mathbb{R}^2} \frac{\hat{g}(x,y)}{xy}\,dx\,dy.$$

(1) Knowing the zeros of the functions $L(s,\chi)$

(2) Discretizing the integral

(3) Dealing with the Principal Value

(4) Restricting the range of integration

(5) Truncating the infinite products hiding in $\hat{g}(x,y)$

Knowing the zeros of the functions $L(s,\chi)$

In 1993 Rumely published his calculations of zeros of Dirichlet L-functions to all moduli $3 \le q \le 100$ (and more).

He calculated all of the zeros in the critical strip $0 < \operatorname{Re} s < 1$ satisfying $|\operatorname{Im} s| \le 2500$, and for small moduli (including $q = 12$) went up to at least $|\operatorname{Im} s| \le 10000$.

(All of them happened to have $\operatorname{Re} s = \frac{1}{2}$, by the way.)

Discretizing the integral

We choose $\varepsilon > 0$ and use the approximation

$$\iint_{\mathbb{R}^2} \frac{\hat{g}(x,y)}{xy}\,dx\,dy \approx \varepsilon^2 \sum_{\substack{m,n\in\mathbb{Z}\\ m,n \text{ odd}}} \frac{\hat{g}(m\varepsilon/2, n\varepsilon/2)}{(m\varepsilon/2)(n\varepsilon/2)}.$$

If $f(x,y) = \hat{g}(x,y)/xy$, that the Poisson summation formula gives

$$\varepsilon^2 \sum_{\substack{m,n\in\mathbb{Z}\\ m,n \text{ odd}}} f(m\varepsilon/2, n\varepsilon/2) = \hat{f}(0,0) + \sum_{\substack{k,l\in\mathbb{Z}\\ (k,l)\neq(0,0)}} \hat{f}(2\pi k/\varepsilon, 2\pi l/\varepsilon)(-1)^{k+l}.$$

The main term is $\hat{f}(0,0) = \iint_{\mathbb{R}^2} \frac{\hat{g}(x,y)}{xy}\,dx\,dy$.

The other $\hat{f}$ terms can be translated into quantities involving $g(x,y)$, which are subsequently estimated using quantitative forms of the Law of Large Numbers.

Dealing with the Principal Value

We note that

$$\mathrm{PV}\iint_{\mathbb{R}^2}\frac{\hat{g}(x,y)}{xy}\,dx\,dy=\mathrm{PV}\iint_{\mathbb{R}^2}\frac{\hat{g}(x,y)-\hat{g}(x,0)\hat{g}(0,y)}{xy}\,dx\,dy$$

since $\hat{g}$ is an even function of each variable separately.

The new integrand can be extended continuously to the coordinate axes, and can itself be shown to be an integrable function (not trivial in more than one dimension!).

Therefore the PV on the right-hand side can be removed, and the Poisson summation formula truly applies, giving

$$\begin{aligned}
&\iint_{\mathbb{R}^2}\frac{\hat{g}(x,y)-\hat{g}(x,0)\hat{g}(0,y)}{xy}\,dx\,dy\\
&\qquad\approx\varepsilon^2\sum_{\substack{m,n\in\mathbb{Z}\\ m,n\text{ odd}}}\frac{\hat{g}(m\varepsilon/2,n\varepsilon/2)-\hat{g}(m\varepsilon/2,0)\hat{g}(0,n\varepsilon/2)}{(m\varepsilon/2)(n\varepsilon/2)}\\
&\qquad=\varepsilon^2\sum_{\substack{m,n\in\mathbb{Z}\\ m,n\text{ odd}}}\frac{\hat{g}(m\varepsilon/2,n\varepsilon/2)}{(m\varepsilon/2)(n\varepsilon/2)}=4\sum_{\substack{m,n\in\mathbb{Z}\\ m,n\text{ odd}}}\frac{\hat{g}(m\varepsilon/2,n\varepsilon/2)}{mn},
\end{aligned}$$

again since $\hat{g}$ is even in each variable.

Restricting the range of summation

Changing $\displaystyle\sum_{\substack{m,n\in\mathbb{Z}\\ m,n \text{ odd}}} \frac{\hat g(m\varepsilon/2, n\varepsilon/2)}{mn}$ to $\displaystyle\sum_{\substack{|m|,|n|\le C\\ m,n \text{ odd}}} \frac{\hat g(m\varepsilon/2, n\varepsilon/2)}{mn}$

requires estimating the functions $F(z,\chi)$ for large z.

This follows from the asymptotic formula

$$\#\{0<\gamma<T\colon L(\tfrac12+i\gamma,\chi)=0\} \sim \tfrac{T}{2\pi}\log\tfrac{qT}{2\pi e}$$

(where q is the conductor of χ) and the estimate

$$|J_0(z)| \le \min\left\{1, \sqrt{\tfrac{2}{\pi|z|}}\right\}.$$

Remark: this Bessel function inequality is sharp for infinitely many z. Does anybody know a nice reference for this precise inequality, rather than simply the asymptotic inequality

$$|J_0(z)| \le \sqrt{\tfrac{2+o(1)}{\pi|z|}}\,?$$

Truncating the infinite products

We use the approximation

$$\prod_{\substack{\gamma>0 \\ L(\frac{1}{2}+i\gamma,\chi_D)=0}} J_0\Big(\frac{2z}{\sqrt{1/4+\gamma^2}}\Big) = \prod_{\substack{0<\gamma<T \\ L(\frac{1}{2}+i\gamma,\chi_D)=0}} J_0\Big(\frac{2z}{\sqrt{1/4+\gamma^2}}\Big) \times \prod_{\substack{\gamma>T \\ L(\frac{1}{2}+i\gamma,\chi_D)=0}} J_0\Big(\frac{2z}{\sqrt{1/4+\gamma^2}}\Big)$$

$$= \prod_{\substack{0<\gamma<T \\ L(\frac{1}{2}+i\gamma,\chi_D)=0}} J_0\Big(\frac{2z}{\sqrt{1/4+\gamma^2}}\Big) \times \big(1 - b_1(\chi,T)z^2 + O(z^4)\big),$$

where we have defined

$$b_1(\chi,T) = \sum_{\substack{\gamma>T \\ L(\frac{1}{2}+i\gamma,\chi_D)=0}} \frac{1}{1/4+\gamma^2}.$$

Luckily, we have the classical formula

$$2b_1(\chi,0) = \log\frac{q}{\pi} - c_\chi + 2\,\mathrm{Re}\,\frac{L'(1,\chi)}{L(1,\chi)}$$

where c_χ is a constant depending only on whether $\chi(-1)$ equals 1 or -1. There are closed-form formulas for $L(1,\chi)$ and $L'(1,\chi)$, and hence $b_1(\chi,T)$ and our approximation can be computed from Rumely's list of zeros up to height T.