Inequities in the Shanks-Rényi prime number race

Greg Martin
University of British Columbia

25th Journées Arithmétiques
King's Buildings, University of Edinburgh
July 2, 2007

3	7	11	19	23

5	13	17	29

Primes up to 30, sorted by residue class modulo 4

3	7	11	19	23	31	43	47	59

5	13	17	29	37	41	53

Primes up to 60, sorted by residue class modulo 4

3	7	11	19	23	31	43	47	59	67	71	79	83

5	13	17	29	37	41	53	61	73	89

Primes up to 90, sorted by residue class modulo 4

3	7	11	19	23	31	43	47	59	67	71	79	83	103	107

5	13	17	29	37	41	53	61	73	89	97	101	109

Primes up to 120, sorted by residue class modulo 4

3	7	11	19	23	31	43	47	59	67	71	79	83	103	107	127	131	139

5	13	17	29	37	41	53	61	73	89	97	101	109	113	137

Primes up to 150, sorted by residue class modulo 4

Races where such advantages are observed:

- Primes that are 2 (mod 3) over primes that are 1 (mod 3)
- Primes that are 3 (mod 4) over primes that are 1 (mod 4)
- Primes that are 2 or 3 (mod 5) over primes that are 1 or 4 (mod 5)
- Primes that are 3, 5, or 6 (mod 7) over primes that are 1, 2, or 4 (mod 7)
- Primes that are 3, 5, or 7 (mod 8) over primes that are 1 (mod 8)
- ...

The general pattern:

Primes that are nonsquares (mod q) over primes that are squares (mod q)

Races where such advantages are observed:

- Primes that are 2 (mod 3) over primes that are 1 (mod 3)
- Primes that are 3 (mod 4) over primes that are 1 (mod 4)
- Primes that are 2 or 3 (mod 5) over primes that are 1 or 4 (mod 5)
- Primes that are 3, 5, or 6 (mod 7) over primes that are 1, 2, or 4 (mod 7)
- Primes that are 3, 5, or 7 (mod 8) over primes that are 1 (mod 8)
- ...

The general pattern:

Primes that are nonsquares (mod q) over primes that are squares (mod q)

Lothian 3 / 7 / 8 / 9 / 29 / 31 / 37 / 49

Further computation (1950s and beyond) reveals that there are moments of triumph for the square residue classes over nonsquare residue classes:

$$\pi(x; q, a) = \{\text{the number of primes } p \leq x \text{ such that } p \equiv a \pmod{q}\}$$

- $\pi(x; 4, 1) > \pi(x; 4, 3)$ for the first time at $x = 26{,}861$
- $\pi(x; 8, 1) > \pi(x; 8, 5)$ for the first time at $x = 588{,}067{,}889$ (although $\pi(x; 8, 1)$ still lags behind $\pi(x; 8, 3)$ and $\pi(x; 8, 7)$)
- $\pi(x; 3, 1) > \pi(x; 3, 2)$ for the first time at $x = 608{,}981{,}813{,}029$

And theoretical results as well:

- The prime number theorem for arithmetic progressions ($1900 + O(1)$): $\pi(x; q, a) \sim \pi(x; q, b)$
- Littlewood (1910s): each of $\pi(x; 4, 1)$ and $\pi(x; 4, 3)$ is ahead of the other for arbitrarily large x, and similarly for $\pi(x; 3, 1)$ and $\pi(x; 3, 2)$
- Turán and Knapowski (1960s): $\pi(x; q, a)$ is ahead of $\pi(x; q, b)$ for arbitrarily large x, for many pairs of residue classes a, b. However, assumptions on the locations of zeros of Dirichlet L-functions are appearing.
- Kaczorowski (1990s): further results in this vein and also for "3-way races", "4-way races", etc.

So the question is:

How often is $\pi(x;q,a)$ ahead of $\pi(x;q,b)$?

Define $\delta_{q;a,b}$ to be the logarithmic density of the set of real numbers $x \geq 1$ satisfying $\pi(x;q,a) > \pi(x;q,b)$. More explicity,

$$\delta_{q;a,b} = \lim_{X\to\infty} \left(\frac{1}{\log X} \int\limits_{\substack{1\leq x\leq X \\ \pi(x;q,a)>\pi(x;q,b)}} \frac{dx}{x} \right).$$

Most important to remember:

> $\delta_{q;a,b}$ measures the limiting "probability" that when a "random" real number x is chosen, there are more primes that are congruent to $a \pmod q$ up to x then there are congruent to $b \pmod q$.

Rubinstein and Sarnak (1994) investigated these densities under the following two hypotheses:

- The Generalized Riemann Hypothesis (GRH): all nontrivial zeros of Dirichlet L-functions have real part equal to $\frac{1}{2}$

Note: Recent work of Ford and Konyagin shows that certain hypothetical violations of GRH do actually lead to pathological behavior in prime number races.

Rubinstein and Sarnak (1994) investigated these densities under the following two hypotheses:

- The Generalized Riemann Hypothesis (GRH): all nontrivial zeros of Dirichlet L-functions have real part equal to $\frac{1}{2}$
- A linear independence hypothesis (LI): the nonnegative imaginary parts of these nontrivial zeros are linearly independent over the rationals

Note: The linear independence hypothesis is somewhat analogous to a "nonsingularity" hypothesis: if we had precise information about any linear dependences that might exist, we could probably still work out the answer....

$\delta_{q;a,b}$: the "probability" that $\pi(x;q,a) > \pi(x;q,b)$

Under these two hypotheses, the Generalized Riemann Hypothesis (GRH) and the linear independence hypothesis (LI), Rubinstein and Sarnak proved:

- $\delta_{q;a,b}$ always exists and is strictly between 0 and 1
- $\delta_{q;a,b} + \delta_{q;b,a} = 1$
- $\delta_{q;a,b} > \frac{1}{2}$ if and only if a is a nonsquare (mod q) and b is a square (mod q)
- if a and b are distinct squares (mod q) or distinct nonsquares (mod q), then $\delta_{q;a,b} = \delta_{q;b,a} = \frac{1}{2}$
- $\delta_{q;a,b}$ tends to $\frac{1}{2}$ as q tends to infinity, uniformly for all pairs a, b of distinct reduced residues (mod q).

$\delta_{q;a,b}$: the "probability" that $\pi(x;q,a) > \pi(x;q,b)$

In joint work with A. Feuerverger (2000), we extended Rubinstein and Sarnak's new approach in several directions. For example, we calculated (assuming, as usual, GRH and LI) many examples of the densities $\delta_{q;a,b}$.

The calculations involved generalizing the formulas of Rubinstein and Sarnak, followed by numerical evaluation of complicated integrals involving many zeros of Dirichlet L-functions.

One significant discovery is that even with q fixed, the values of $\delta_{q;a,b}$ vary significantly as a and b vary over squares and nonsquares (mod q).

$\delta_{q;a,b}$: the "probability" that $\pi(x;q,a) > \pi(x;q,b)$

Examples for the moduli $q = 24$ and $q = 43$:

a	$\delta_{24;a,1}$
5	0.999987
11	0.999983
23	0.999889
7	0.999833
19	0.999719
17	0.999125
13	0.998722

a	a^{-1} (43)	$\delta_{43;a,1}$
30	33	0.57044
32	39	0.57039
12	18	0.56904
20	28	0.56881
19	34	0.56613
8	27	0.56606

a	a^{-1} (43)	$\delta_{43;a,1}$
5	26	0.56366
7	37	0.56345
2	22	0.56281
3	29	0.56065
42	42	0.55982

Note: we did establish some equalities between certain $\delta_{q;a,b}$:

- $\delta_{q;a,b} = \delta_{q;ab^{-1},1}$ for any square $b \pmod q$. Thus it suffices to calculate only the values of $\delta_{q;a,1}$ for nonsquares $a \pmod q$.
- $\delta_{q;a,1} = \delta_{q;a^{-1},1}$ for any $a \pmod q$.

Current goals:

• A more precise understanding of the sizes of $\delta_{q;a,b}$. Recalling that $\delta_{q;a,b}$ tends to $\frac{1}{2}$ as q tends to infinity, we would like an asymptotic formula for $\delta_{q;a,b} - \frac{1}{2}$, for example.

• A way to decide which $\delta_{q;a,b}$ are likely to be larger than others as a and b vary (with q fixed), based on elementary criteria rather than laborious numerical calculation.

$\delta_{q;a,b}$: the "probability" that $\pi(x;q,a) > \pi(x;q,b)$

Theorem (M., 2007+), version I. Assume GRH and LI. If a is a nonsquare (mod q) and b is a square (mod q), then

$$\delta_{q;a,b} = \frac{1}{2} + \frac{\rho(q)}{2\sqrt{\pi}\,(\phi(q)\log q)^{1/2}} + O\Big(\frac{\rho(q)\log\log q}{\phi(q)^{1/2}(\log q)^{3/2}}\Big).$$

In particular, we have

$$\delta_{q;a,b} = \frac{1}{2} + O_\varepsilon\left(\frac{1}{q^{1/2-\varepsilon}}\right)$$

for any $\varepsilon > 0$.

$\rho(q)$ = the number of square roots of 1 (mod q)

$= 2^{\#\text{number of odd prime factors of } q} \times \{1, 2, \text{ or } 4\}$

$\delta_{q;a,b}$: the "probability" that $\pi(x;q,a) > \pi(x;q,b)$

Theorem (M., 2007+), version II. Assume GRH and LI. If a is a nonsquare (mod q) and b is a square (mod q), then

$$\delta_{q;a,b} = \frac{1}{2} + \frac{\rho(q)}{\sqrt{2\pi V(q;a,b)}} + O\Big(\frac{1}{\phi(q)\log q}\Big),$$

where

$$V(q;a,b) = 2 \sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0}} |\chi(b) - \chi(a)|^2 \sum_{\substack{\gamma > 0 \\ L(\frac{1}{2}+i\gamma,\chi)=0}} \frac{1}{\frac{1}{4}+\gamma^2}\,.$$

$\delta_{q;a,b}$: the "probability" that $\pi(x;q,a) > \pi(x;q,b)$

Theorem (M., 2007+), version III. Assume GRH and LI. If a is a nonsquare (mod q) and b is a square (mod q), then

$$\delta_{q;a,b} = \frac{1}{2} + \frac{\rho(q)}{\sqrt{2\pi V(q;a,b)}} + O\Big(\frac{1}{\phi(q)\log q}\Big),$$

where

$$V(q;a,b) = 2 \sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0}} |\chi(b) - \chi(a)|^2 \sum_{\substack{\gamma > 0 \\ L(\frac{1}{2}+i\gamma,\chi)=0}} \frac{1}{\frac{1}{4}+\gamma^2}$$

$$= 2\phi(q)\Big(\log q - \sum_{p \mid q} \frac{\log p}{p-1} - (\gamma_0 + \log 2\pi) + R_q(a-b) \Big)$$

$$+ (2\log 2)\iota_q(-ab^{-1})\phi(q) + 2M(q;a,b).$$

$$V(q;a,b) = 2\phi(q)\left(\log q - \sum_{p|q}\frac{\log p}{p-1} - (\gamma_0 + \log 2\pi) + R_q(a-b)\right)$$
$$+ (2\log 2)\iota_q(-ab^{-1})\phi(q) + 2M(q;a,b).$$

There are three terms in this formula for the variance $V(q;a,b)$ that depend on a and b. Whenever any of the three is bigger than normal, the variance increases, causing the density $\delta_{q;a,b}$ to decrease.

$$V(q;a,b) = 2\phi(q)\left(\log q - \sum_{p\mid q}\frac{\log p}{p-1} - (\gamma_0 + \log 2\pi) + R_q(a-b)\right)$$
$$+ (2\log 2)\iota_q(-ab^{-1})\phi(q) + 2M(q;a,b).$$

- $\iota_q(n) = \begin{cases} 1, & \text{if } n \equiv 1 \pmod q, \\ 0, & \text{if } n \not\equiv 1 \pmod q \end{cases}$
- $R_q(n) = \dfrac{\Lambda(q/(q,n))}{\phi(q/(q,n))}$
- $M(q;a,b) = \displaystyle\sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0}} |\chi(a) - \chi(b)|^2 \frac{L'(1,\chi^*)}{L(1,\chi^*)}$, where χ^* is the primitive character that induces χ
- $\gamma_0 =$ Euler's constant: $\displaystyle\lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n} - \log x\right) \approx 0.577216$

$$R_q(a-b) = \frac{\Lambda(q/(q,a-b))}{\phi(q/(q,a-b))}$$

provides extra variance (which reduces the corresponding density $\delta_{q;a,b}$) if a is congruent to b modulo appropriately large divisors of q:

$$R_q(a-b) = \frac{\Lambda(q/(q,a-b))}{\phi(q/(q,a-b))}$$

provides extra variance (which reduces the corresponding density $\delta_{q;a,b}$) if a is congruent to b modulo appropriately large divisors of q:

a	$\delta_{24;a,1}$	$24/(24,a-1)$	$R_{24}(a-1)$
5		6	0
11		12	0
23		12	0
7		4	$(\log 2)/2$
19		4	$(\log 2)/2$
17		3	$(\log 3)/2$
13		2	$\log 2$

$$R_q(a-b) = \frac{\Lambda(q/(q,a-b))}{\phi(q/(q,a-b))}$$

provides extra variance (which reduces the corresponding density $\delta_{q;a,b}$) if a is congruent to b modulo appropriately large divisors of q:

a	$\delta_{24;a,1}$	$24/(24,a-1)$	$R_{24}(a-1)$
5	0.999987	6	0
11	0.999983	12	0
23	0.999889	12	0
7	0.999833	4	$(\log 2)/2$
19	0.999719	4	$(\log 2)/2$
17	0.999125	3	$(\log 3)/2$
13	0.998722	2	$\log 2$

$$\iota_q(-ab^{-1}) = \begin{cases} 1, & \text{if } -ab^{-1} \equiv 1 \pmod{q}, \\ 0, & \text{if } -ab^{-1} \not\equiv 1 \pmod{q} \end{cases}$$

$$M(q;a,b) = \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} |\chi(a) - \chi(b)|^2 \frac{L'(1,\chi^*)}{L(1,\chi^*)}$$

$\iota_q(-ab^{-1})$ provides extra variance exactly when $a \equiv -b \pmod{q}$. It can be shown that $M(q;a,b)$ tends to provide extra variance when there are small primes congruent to ab^{-1} and/or ba^{-1} modulo q.

(Note: the last sentence above becomes a bit more complicated to state when q is not an odd prime power.)

$\iota_q(-ab^{-1})$ provides extra variance exactly when $a \equiv -b \pmod{q}$. It can be shown that $M(q; a, b)$ tends to provide extra variance when there are small primes congruent to ab^{-1} and/or ba^{-1} modulo q.

a	$a^{-1} \pmod{43}$	$\delta_{43;a,1} = \delta_{43;a^{-1},1}$
30	33	
32	39	
12	18	
20	28	
19	34	
8	27	
5	26	
7	37	
2	22	
3	29	
42	42	

$\iota_q(-ab^{-1})$ provides extra variance exactly when $a \equiv -b \pmod{q}$. It can be shown that $M(q; a, b)$ tends to provide extra variance when there are small primes congruent to ab^{-1} and/or ba^{-1} modulo q.

a	$a^{-1} \pmod{43}$	$\delta_{43;a,1} = \delta_{43;a^{-1},1}$
30	33	0.57044
32	39	0.57039
12	18	0.56904
20	28	0.56881
19	34	0.56613
8	27	0.56606
5	26	0.56366
7	37	0.56345
2	22	0.56281
3	29	0.56065
42	42	0.55982

Inequities in the Shanks-Rényi prime number race

Greg Martin
University of British Columbia

slides available at:
http://www.math.ubc.ca/∼gerg/index.shtml?slides