On the number of $\mathbb{F}_p$-valued points of elliptic curves

Kyushu University

Shinnya Okumura

Outline

$E/\mathbb{Q}$: elliptic curve over $\mathbb{Q}$ defined by a Weierstrass equation with integer coefficients.

p, ℓ : prime number.

$E(\mathbb{F}_p)$: group of $\mathbb{F}_p$-valued points of E mod p.

(E has good reduction at p).

a, b, t : positive integers with GCD(a, b) = 1.

1. Primality of $|E(\mathbb{F}_p)|/t$ when p varies satisfying $p \equiv a \ (mod\ b)$.
2. Divisibility of $|E(\mathbb{F}_p)|$ when p varies satisfying $p \equiv a \ (mod\ b)$.
3. Explanation of our conjecture about primality of $|E(\mathbb{F}_p)|/t$.
4. Three examples.

Primality of $|E(\mathbb{F}_p)|/t$

$P := \{p : prime\}$

$S_E := \{p \in P | E\ has\ bad\ reduction\ at\ p\}$

$\pi_{E,t}(x) := |\{p \leq x | p \in P \setminus S_E\ and\ |E(\mathbb{F}_p)|/t\ is\ prime\}|$

Conjecture1 (Zywina)

$$\pi_{E,t}(x) \sim C_{E,t} \frac{x}{(\log x)^2}$$

as $x \to \infty$, where $C_{E,t}$ is a constant depending on E and t.

※Zywina generalized it to the number field case.

Zywina tested his conjecture for some elliptic curves and got better results than Koblitz's conjecture.

We try to refine Zywina's conjecture. More precisely, we consider a next problem.

Are there any conditions of p that $\left|E\left(\mathbb{F}_p\right)\right|/t$ is apt to become prime ?

We find that the probability that $\left|E\left(\mathbb{F}_p\right)\right|/t$ is prime varies with *a* if we impose the congruence condition $p \equiv a\ (mod\ b)$ by testing for some elliptic curves.

So we consider the conditional probability

$$P\left(\left|E\left(\mathbb{F}_p\right)\right|/t \text{ is prime } \middle| p \equiv a(mod\ b)\right)$$

Our conjecture about primality of $\left|E\left(\mathbb{F}_p\right)\right|/t$

$\Sigma_{a,b} := \{p \in P | p \equiv a (mod\ b)\}$

$\pi_{a,b}(x) := \left|\left\{p \leq x | p \in \Sigma_{a,b}\right\}\right|$

$\pi_{E,\,t,\,a,b}(x) :=$

$\left|\left\{p \leq x \middle| p \in \Sigma_{a,b} \setminus S_E \ \ and \left|E\left(\mathbb{F}_p\right)\right|/t \ is \ prime\right\}\right|$

Conjecture2

$$P_E(t,a,b,x) := \frac{\pi_{E,\,t,\,a,b}(x)}{\pi_{a,b}(x)} \sim C_{E,t} C_{E,t,a,b} \frac{1}{\log x}$$

as $x \to \infty$, where $C_{E,t}$ is the constant which occurs in Zywina's conjecture, and $C_{E,t,a,b}$ is a constant depending on E, t, a and b.

Remark

Zywina used the following integral to calculate the value of $\pi_{E,t}(x)$.

$$\pi_{E,t}(x) \sim C_{E,t} \int_{t+1}^{x} \frac{1}{\log(u+1)-\log t} \frac{du}{\log u} \quad \text{as } x \to \infty.$$

Zywina's heuristics suggest that this will be a better approximation of $\pi_{E,t}(x)$ than $C_{E,t} \frac{x}{(\log x)^2}$.

Thus we use the following expression to calculate the expected value of $P_E(t, a, b, x)$.

$$P_E(t, a, b, x) \sim \frac{C_{E,t} C_{E,t,a,b} \int_{t+1}^{x} \frac{1}{\log(u+1)-\log t} \frac{du}{\log u}}{\pi(x)}$$

as $x \to \infty$, where $\pi(x) := |\{p \leq x | p \in P\}|$.

Divisibility of $\left|E\left(\mathbb{F}_p\right)\right|$

In addition we also consider the divisibility of $\left|E\left(\mathbb{F}_p\right)\right|$. More precisely, we consider whether or not for a given E, there is a triple $(a, b, \ell) \in \mathbb{Z}^3$ wit GCD$(a, b) = 1$ such that $\left|E\left(\mathbb{F}_p\right)\right|$ is divisible by some prime ℓ if $p \equiv a(mod\ b)$.

About this, we prove the next theorem.

Theorem3

Δ_E: discriminant of E.

f_E:conductor of $\mathbb{Q}\left(\sqrt{\Delta_E}\right)$.

Suppose that E is not $\mathbb{Q}$-isogenous to an elliptic curve which has non-trivial $\mathbb{Q}$-torsion points.

(i). If $\sqrt{\Delta_E} \notin \mathbb{Q}$, then there are integers $a_1, a_2, \ldots, a_{\frac{\varphi(f_E)}{2}}$ with $a_i \not\equiv a_j (mod\ f_E)(i \neq j)$ such that $\left|E\left(\mathbb{F}_p\right)\right|$ is divisible by 2 if $p \in \Sigma_{a_i, f_E} \setminus S_E$ and $p \nmid 2f_E$ for $i = 1,2, \ldots \frac{\varphi(f_E)}{2}$, where $\varphi(\cdot)$ is the Euler function.

(ii). If $\sqrt{\Delta_E} \in \mathbb{Q}$ and F_E is the conductor of $\mathbb{Q}(E[2])$, then there are integers $a_1, a_2, \ldots, a_{\frac{\varphi(F_E)}{3}}$ with $a_i \not\equiv a_j (mod\ F_E)(i \neq j)$ such that $\left|E\left(\mathbb{F}_p\right)\right|$ is divisible by 2 if $p \in \Sigma_{a_i,F_E} \setminus S_E$ and $p \nmid 2F_E$ for $i = 1,2, \ldots \frac{\varphi(F_E)}{3}$, where the field $\mathbb{Q}(E[2])$ is obtained from $\mathbb{Q}$ by adjoining the coordinates of all points of $E[2]$.

Explanation of our conjecture

If $\left|E\left(\mathbb{F}_p\right)\right|/t$ behaves like a random integer when p varies, by the prime number theorem

$\left|E\left(\mathbb{F}_p\right)\right|/t$ is prime with probability

$$\frac{1}{\log\left|E\left(\mathbb{F}_p\right)\right|/t} = \frac{1}{\log\left|E\left(\mathbb{F}_p\right)\right|-\log t} \approx \frac{1}{\log(p+1)-\log t}.$$

But $\left|E\left(\mathbb{F}_p\right)\right|/t$ do not behave like a random integer (e.g. Sato-Tate conjecture). So the above probability should be corrected as following :

$$C\,\frac{1}{\log(p+1)-\log t}\,.$$

The constant C is called a correction factor.

We should define C as if it shows how often $\left|E(\mathbb{F}_p)\right|/t$ becomes prime than a random integer, when p varies.

Then $\pi_{E,\,t}(x)$ can be expected as follows:

$$\sum_{\substack{p\notin S_E \\ t\le p\le x}} C\frac{1}{\log(p+1)-\log t}$$

$$\sim C\int_{t+1}^{x}\frac{1}{\log(u+1)-\log t}\frac{du}{\log u}$$

$$\sim C\frac{x}{(\log x)^2} \qquad (x\ \to\infty).$$

We should define $C_{E,\,t,\,a,\,b}$ as if it shows how often $\left|E(\mathbb{F}_p)\right|/t$ becomes prime than the unconditional case, when p varies with $p \equiv a \pmod{b}$.

$\pi_{E,\,t,\,a,b}(x)$ can be expected as follows:

$$\frac{1}{\varphi(b)} \sum_{\substack{p \notin S_E \\ t \le p \le x}} C_{E,\,t,\,a,\,b} C \frac{1}{\log(p+1) - \log t}$$

$$\sim \frac{1}{\varphi(b)} C_{E,\,t,\,a,\,b} C \int_{t+1}^{x} \frac{1}{\log(u+1) - \log t} \frac{du}{\log u}$$

$$\sim \frac{1}{\varphi(b)} C_{E,\,t,\,a,\,b} C \frac{x}{(\log x)^2} \qquad (x \to \infty).$$

1. Zywina's heuristics

First, we recall some facts about a Galois representation attached to torsion subgroups of E.

$$\rho_m : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}) =: G_m$$

$G(m) := \mathrm{Im}\rho_m \cong \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$

Frob_p : Frobenius conjugacy class at p.

Then, if $p \nmid m$, p *is unramified in* $\mathbb{Q}(E[m])$ and

$|E(\mathbb{F}_p)| \equiv \det(I - \rho_m(\mathrm{Frob}_p))$

$= \det(\rho_m(\mathrm{Frob}_p)) + 1 - \mathrm{Tr}(\rho_m(\mathrm{Frob}_p)) \pmod{m}$

Moreover, we recall the Chebotarev density theorem.

Theorem4(Chebotarev)

Let L/K be a (finite) Galois extension of number fields and let $\mathcal{C} \subseteq \mathrm{Gal}(L/K)$ be any subset which is stable by $\mathrm{Gal}(L/K)$-conjugation. Let P_K be the set of prime ideals of $\mathcal{O}_K$ where $\mathcal{O}_K$ is the ring of integers of K, and let $P_K(x)$ be the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ such that $N_K(\mathfrak{p}) \leq x$. For each $\mathfrak{p} \in P_K$ which is unramified in L, let $\mathrm{Frob}_{\mathfrak{p}} \subseteq \mathrm{Gal}(L/K)$ denote the conjugacy class of the Frobenius element attached to any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$. Then

$$\lim_{x\to\infty} \frac{\left|\left\{\mathfrak{p} \in P_K(x) \middle| \mathfrak{p}\ is\ unramified\ in\ L\ and \mathrm{Frob}_{\mathfrak{p}} \subseteq \mathcal{C}\right\}\right|}{|P_K(x)|}$$

$$= \frac{|\mathcal{C}|}{|\mathrm{Gal}(L/K)|}.$$

Zywina define a next set

$$\psi_t(m) \coloneqq \left\{A \in G(m) \middle| \det(I - A) \in t \cdot (\mathbb{Z}/m\mathbb{Z})^{\times}\right\}.$$

The Chebotarev density theorem implies that when m is divisible by $t \prod_{\ell \mid t} \ell$,

$$\delta_{E,t}(m) \coloneqq \frac{|\psi_t(m)|}{|G(m)|}$$

is the probability that for a random $p \in P \setminus S_E$, $\left|E(\mathbb{F}_p)\right|/t$ is an integer and invertible mod m.

On the other hand, the probability that a random natural number is invertible mod m is $\prod_{\ell|m}(1-\frac{1}{\ell})$.

He expected

$$\frac{\delta_{E,t}(m)}{\prod_{\ell|m}(1-\frac{1}{\ell})}\frac{1}{\log(p+1)-\log t}$$

to be a better approximation for $P\left(\left|E\left(\mathbb{F}_p\right)\right|/t \text{ is prime } \middle| p : prime\right)$ and defined $C_{E,\,t}$ as follows:

$$C_{E,\,t} := \lim_{z\to\infty}\frac{\delta_{E,t}(t\prod_{\ell\leq z}\ell)}{\prod_{\ell\leq z}(1-\frac{1}{\ell})}$$

2. Our heuristics

We define

$\psi_{t,a,b}(m) :=$
$\{A \in \psi_t(m) | \det(A \bmod \ell^n) = a \text{ for all } \ell^n \parallel \gcd(m,b)\}.$

$G_{a,t}(m) := \{A \in \psi_t(m) | \det A = a\}.$

$b = \prod_{\ell|b} \ell^{r(\ell)}$. (decomposition into prime factors)

$m(z) := \prod_{\ell \le z} \ell^{r(\ell)}$ (if $\ell \nmid b$, $r(\ell) = 1$).

If $z > t, b$, $\frac{|\psi_{t,a,b}(tm(z))|}{|G(tm(z))|}$ is the probability that

for a random $p \in P \setminus S_E$, $\left|E(\mathbb{F}_p)\right|/t$ is an integer, relatively prime to $m(z)$ and $p \equiv a \pmod b$.

We define $C_{E,\,t,\,a,\,b}$ as follows:

$$C_{E,\,t,\,a,\,b} := \lim_{z\to\infty} \frac{\dfrac{\varphi(b)\left|\psi_{t,\,a,\,b}(tm(z))\right|}{\left|G\left(tm(z)\right)\right|}}{\delta_{E,t}(tm(z))}.$$

※If E has complex multiplication, we define $C_{E,\,t,\,a,\,b}$ by a different way, because it is convenient for calculation of it.

Calculation of $C_{E,\,t,\,a,\,b}$ (non-CM case)

Assume that E does not have complex multiplication.

Theorem5(Serre)

There is a constant $M := M_E$ depending on E such that if m and n are positive integers with $\gcd(n, mM) = 1$, then

$$G(mn) \cong G(m) \times \mathrm{Aut}(E[n]).$$

From now on we assume $\gcd(b, Mt) = 1$.

From this theorem, we may identify $\psi_{t,\,a,\,b}(tm(z))$ with the direct product set

$$\prod_{\ell \mid b,} G_{a,\,t}\left(\ell^{r(\ell)}\right) \times \prod_{\ell \nmid bMt} \psi_t(\ell) \times \psi_t\left(t \prod_{\ell \mid Mt} \ell\right),$$

where ℓ runs over all $\ell | m(z)$. It is easy to see that

If $\ell \nmid Mt$, then $G(\ell^n) = G_{\ell^n}$ and

$$\frac{|G_{a,t}(\ell^n)|}{|\psi_t(\ell^n)|} = \frac{\ell^{3(n-1)}|G_{a,t}(\ell)|}{\ell^{4(n-1)}|\psi_t(\ell)|} = \frac{|G_{a,1}(\ell)|}{\ell^{(n-1)}|\psi_1(\ell)|}.$$

Thus we have

$$\begin{aligned} C_{E,t,a,b} &= \lim_{z\to\infty} \frac{\varphi(b)|\psi_{t,a,b}(tm(z))|}{|\psi_t(tm(z))|} \\ &= \prod_{\ell|b} (\ell^{r(\ell)} - \ell^{(r(\ell)-1)}) \frac{|G_{a,t}(\ell^{r(\ell)})|}{|\psi_t(\ell^{r(\ell)})|} \\ &= \prod_{\ell|b} (\ell - 1) \frac{|G_{a,1}(\ell)|}{|\psi_1(\ell)|}. \end{aligned}$$

Lemma6

If $\gcd(b, Mt) = 1$,

$$C_{E,\,t,\,a,\,b} = \prod_{\ell \mid b} C_{E,\,1,\,a,\ell}\,.$$

Theorem7

If $\gcd(b, Mt) = 1$, then $C_{E,\,t,\,a,\,b}$ can be calculated as follows:

$$C_{E,t,a,b} = \begin{cases} \prod_{\ell \mid b} \frac{(\ell-1)\left(\ell^2-\ell-1\right)}{\ell^3-2\ell^2-\ell+3} & if\ a = 1, \\ \prod_{\ell \mid b} \frac{(\ell-2)\left(\ell^2-1\right)}{\ell^3-2\ell^2-\ell+3} & if a \neq 1. \end{cases}$$

Calculation of $C_{E,\,t,\,a,\,b}$ (CM case)

Theorem8(Serre)

K : number field.

E_K/K : elliptic curve defined over K with complex multiplication.

$R \coloneqq \mathrm{End}_{\overline{K}}(E_K)$.

Assume that all the elements of R are defined over K.

Then there is a constant $M \coloneqq M_{E_K}$ depending on E_K such that if m and n are positive integers with $\gcd(n, mM) = 1$, then

$$G(mn) \cong G(m) \times \left({}^{R}/_{nR}\right)^{\times}.$$

Assume that E has complex multiplication.

$R \coloneqq \mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathbb{Z} + \mathbb{Z}f\alpha.$

$F \coloneqq R \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}(\sqrt{D})$ (D : square-free integer)

$$\alpha = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \pmod 4, \\ \dfrac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

$d_F : Disc(F).$

$P_F \coloneqq \{prime\ ideal\ of \mathcal{O}_F\}.$

$(\mathcal{O}_F : The\ ring\ of integer\ of\ F)$

Not all the elements of R are defined over $\mathbb{Q}$.

⇒ We consider E as an elliptic curve over F and denote this curve by E_F.

$\Sigma_{F,a,b}^{\mathrm{split}} \coloneqq$

$\{p \in P \setminus S_E \mid p \equiv a\ (mod\ b), p\ splits\ completely\ in\ F\}.$

$$\Sigma_{F,a,b}^{\text{split}}(x) :=$$

$$\left\{\mathfrak{p} \in P_F \mid \mathfrak{p} \cap \mathbb{Z} = (p),\ p \in \Sigma_{F,a,b}^{\text{split}} \text{ and } N_F(\mathfrak{p}) \leq x\right\}.$$

$$\pi_{E_F,\,t,\,a,\,b}^{\text{split}}(x)$$

$$:= \left|\left\{\mathfrak{p} \in \Sigma_{F,a,b}^{\text{split}}(x) - S_{E_F} \mid |E(\mathbb{F}_{\mathfrak{p}})|/t \text{ is prime}\right\}\right|.$$

$$\pi_{E,\,F,t,\,a,\,b}^{\text{split}}(x)$$

$$:= \left|\left\{p \in \Sigma_{F,a,b}^{\text{split}} | p \leq x \text{ and } |E(\mathbb{F}_p)|/t \text{ is prime}\right\}\right|.$$

Similarly, we can define $\Sigma_{F,a,b}^{\text{inert}}$, $\Sigma_{F,a,b}^{\text{inert}}(x)$ and $\pi_{E,\,F,t,\,a,\,b}^{\text{inert}}(x)$. Then we have

$$\pi_{E,\,t,\,a,\,b}(x) = \pi_{E,\,F,t,\,a,\,b}^{\text{split}}(x) + \pi_{E,\,F,t,\,a,\,b}^{\text{inert}}(x) + O(1).$$

$$\pi^{\mathrm{split}}_{E,F,t,a,b}(x) = \frac{1}{2}\pi^{\mathrm{split}}_{E_F,t,a,b}(x).$$

Conjecture9

$$\pi^{\mathrm{split}}_{E_F,t,a,b}(x) \sim C^{\mathrm{split}}_{E_F,t,a,b}\pi_{E_F,t}(x) \sim C^{\mathrm{split}}_{E_F,t,a,b}C_{E_F,t}\frac{x}{(\log x)^2}$$

$$\pi^{\mathrm{inert}}_{E,F,t,a,b}(x) \sim C^{\mathrm{inert}}_{t,a,b}\frac{x}{(\log x)^2}\ .$$

$$\pi_{E,t,a,b}(x) \sim \left(\frac{1}{2}C^{\mathrm{split}}_{E_F,t,a,b}C_{E_F,t} + C^{\mathrm{inert}}_{t,a,b}\right)\frac{x}{(\log x)^2}\ .$$

$$(x \longrightarrow \infty)$$

We define $C_{E,t,a,b}$ as follows:

$$C_{E,t,a,b} := \varphi(b)\left(\frac{1}{2}C^{\mathrm{split}}_{E_F,t,a,b}C_{E_F,t} + C^{\mathrm{inert}}_{t,a,b}\right)C_{E,t}{}^{-1}.$$

Note that

$$\frac{|\Sigma_{F,0,1}^{\text{inert}}(x)|}{|\{\mathfrak{p} \in P_F \mid N_F(\mathfrak{p}) \leq x\}|} \longrightarrow 0 \quad (x \longrightarrow \infty).$$

Thus, if $z > t, b,$ then we may consider

$$\frac{|\psi_{t,a,b}(tm(z))|}{|G(tm(z))|}$$

to be the probability that for a random $\mathfrak{p} \in P_F \setminus S_{E_F}$, $|E_F(\mathbb{F}\mathfrak{p})|/t$ is an integer, relatively prime to $m(z)$ and $\mathfrak{p} \cap \mathbb{Z} = (p),\ p \in \Sigma_{F,a,b}^{\text{split}}$. We define

$$C_{E_F,t,a,b}^{\text{split}} := \lim_{z \to \infty} \frac{\frac{|\psi_{t,a,b}(tm(z))|}{|G(tm(z))|}}{\delta_{E_F,t}(tm(z))}.$$

Theorem10 Assume that M is divisible by $\prod_{\ell|2fd_F}\ell$.

If $\ell \nmid Mt$, then $C^{\text{split}}_{E_F,\,t,\,a,\ell^{r(\ell)}}$ can be calculated as follows:

(i)If $\left(\frac{D}{\ell}\right)$=1, then we have

$$C^{\text{split}}_{E_F,\,t,\,a,\ell^{r(\ell)}} = \begin{cases} \frac{1}{\ell^{r(\ell)-1}(\ell-2)} & if\ \ a=1 \\ \frac{\ell-3}{\ell^{r(\ell)-1}(\ell-1)^2} & if\ a\ \neq 1 \end{cases}$$

(ii)If $\left(\frac{D}{\ell}\right)$=-1, then we have

$$C^{\text{split}}_{E_F,\,t,\,a,\ell^{r(\ell)}} = \begin{cases} \frac{\ell}{\ell^{r(\ell)-1}(\ell^2-2)} & if\ \ a=1 \\ \frac{\ell+1}{\ell^{r(\ell)-1}(\ell^2-2)} & if\ a\ \neq 1 \end{cases}$$

Lemma11

$F = \mathbb{Q}(\sqrt{D})$, $(D$: square−free$)$.

f_F: conductor of F.

Then there are integers $a_1, a_2, \ldots, a_{\frac{\varphi(f_F)}{2}}$

$(a_i \not\equiv a_j \pmod{f_F}$ $(i \neq j))$ such that the following holds:

If $p \in P$ and $p \nmid 2f_F D$, then p is inert in F

$\Leftrightarrow p \equiv a_i \pmod{f_F}$ for some $i \in \left\{1,2,\ldots,\frac{\varphi(f_F)}{2}\right\}$.

If p is inert in F, then $|E(\mathbb{F}p)| = p + 1$.

Lemma12

$d \coloneqq \gcd(b, f_F)$.

$J \coloneqq \left\{ i \in \left\{1,2,\ldots,\frac{\varphi(f_F)}{2}\right\} \middle| d|(a - a_i) \right\}$.

$\pi_{t,\alpha,\beta}(x) \coloneqq \left| \left\{ p \leq x \mid p \in P, p \equiv \alpha \pmod{\beta}, \frac{p+1}{t} \text{ is prime} \right\} \right|$.

Then there are integers c_i and ϵ_i such that the following holds:

$$\pi^{\text{inert}}_{E,F,t,a,b}(x) =$$

$$\begin{cases} \sum_{i=1}^{\varphi(f_F)/2} \pi_{t,c_i,bf_F}(x) + O(1) & if \ \ d = 1 \\ \sum_{i \in J} \pi_{t,\epsilon_i,bf'_F}(x) + O(1) & if \ d > 1, f_F = df'_F \end{cases}$$

Conjecture13

There is a constant $C_{\alpha,\beta,t}$ depending of t, α and β such that

$$\pi_{t,\alpha,\beta}(x) \sim \frac{C_{\alpha,\beta,t}}{\varphi(\beta)} \frac{x}{(\log x)^2} \qquad (x \longrightarrow \infty).$$

$C_{\alpha,\beta,t}$ is determined as follows:

$$P\left(\frac{p+1}{t} : prime \middle| p \in P, p \equiv \alpha \pmod{\beta}\right) =$$

$$P(t|(p+1)|p \in P, p \equiv \alpha \pmod{\beta}) \times$$

$$P\left(\frac{p+1}{t} : prime \middle| p \in P, p \equiv \alpha \pmod{\beta}, t|(p+1)\right).$$

$$P\left(\frac{p+1}{t} : prime \middle| p \in P, p \equiv \alpha \pmod{\beta}, t|(p+1)\right)$$
$$\approx P(n : prime) \times$$
$$\prod_{\ell : prime} \frac{P\left(\ell \nmid \frac{p+1}{t} \middle| p \in P, p \equiv \alpha \pmod{\beta}, t|(p+1)\right)}{P(\ell \nmid n)},$$

where $P(n : prime)$ is the probability that a random integer is prime, and $P(\ell \nmid n)$ is the probability that a random integer is not divisible by ℓ.

We define

$$C_{\alpha,\beta,t} := P(t|(p+1)|p \in P, p \equiv \alpha \pmod{\beta}) \times$$
$$\prod_{\ell : prime} \frac{P\left(\ell \nmid \frac{p+1}{t} \middle| p \in P, p \equiv \alpha \pmod{\beta}, t|(p+1)\right)}{P(\ell \nmid n)}.$$

Theorem14 Assume that $\gcd(b, f_F) = 1$.

(i)There are integers c_i such that

$$C_{t,a,b}^{\text{inert}} = \frac{1}{\varphi(bf_F)} \sum_{i=1}^{\frac{\varphi(f_F)}{2}} C_{c_i, bf_F, t}.$$

(ii-i)If $\gcd(bf_F, t) = 1$, there are integers α_i for $i \in \left\{1,2,\ldots,\frac{\varphi(f_F)}{2}\right\}$ such that the following holds:

If $^{\exists}\ell \in P$ such that $\ell | bf_F$ and $t\ell | (\alpha_i + 1)$, then $C_{c_i, bf_F, t} = 0$. Otherwise

$$C_{c_i, bf_F, t} = \begin{cases} \frac{1}{\varphi(t)} \prod_{\ell \nmid bf_F t} \left(1 - \frac{1}{(\ell-1)^2}\right) \prod_{\ell | bf_F} \left(1 + \frac{1}{\ell - 1}\right) & if\ t | (\alpha_i + 1), \\ \frac{1}{\varphi(t)} \prod_{\ell \nmid bf_F t} \left(1 - \frac{1}{(\ell-1)^2}\right) \prod_{\ell | bf_F t} \left(1 + \frac{1}{\ell - 1}\right) & if\ t \nmid (\alpha_i + 1). \end{cases}$$

(ii-ii)If $\gcd(bf_F, t) = e > 1$and $bf_F = ef'$, there are integers β_i for $i \in \left\{1,2,\ldots,\frac{\varphi(f_F)}{2}\right\}$ such that the following holds:

If $e \nmid (c_i + 1)$ or $^{\exists}\ell \in P$ such that $\ell | f'$ and $t\ell | (\beta_i+1)$, then$C_{c_i,bf_F,t} = 0$. Otherwise if $t = t'e$, $\gcd(e, t') = h$ and $t' = t''h$, then we have

$$C_{c_i,bf_F,t} = \begin{cases} \frac{1}{\varphi(t'')h} \prod_{\ell \nmid bf_F t'} \left(1 - \frac{1}{(\ell-1)^2}\right) \prod_{\ell | f'} \left(1 + \frac{1}{\ell - 1}\right) & if\ t | (\beta_i+1), \\ \frac{1}{\varphi(t'')h} \prod_{\ell \nmid bf_F t'} \left(1 - \frac{1}{(\ell-1)^2}\right) \prod_{\ell | bf_F t'} \left(1 + \frac{1}{\ell - 1}\right) & if\ t \nmid (\beta_i+1). \end{cases}$$

Example1 (Non-CM case)

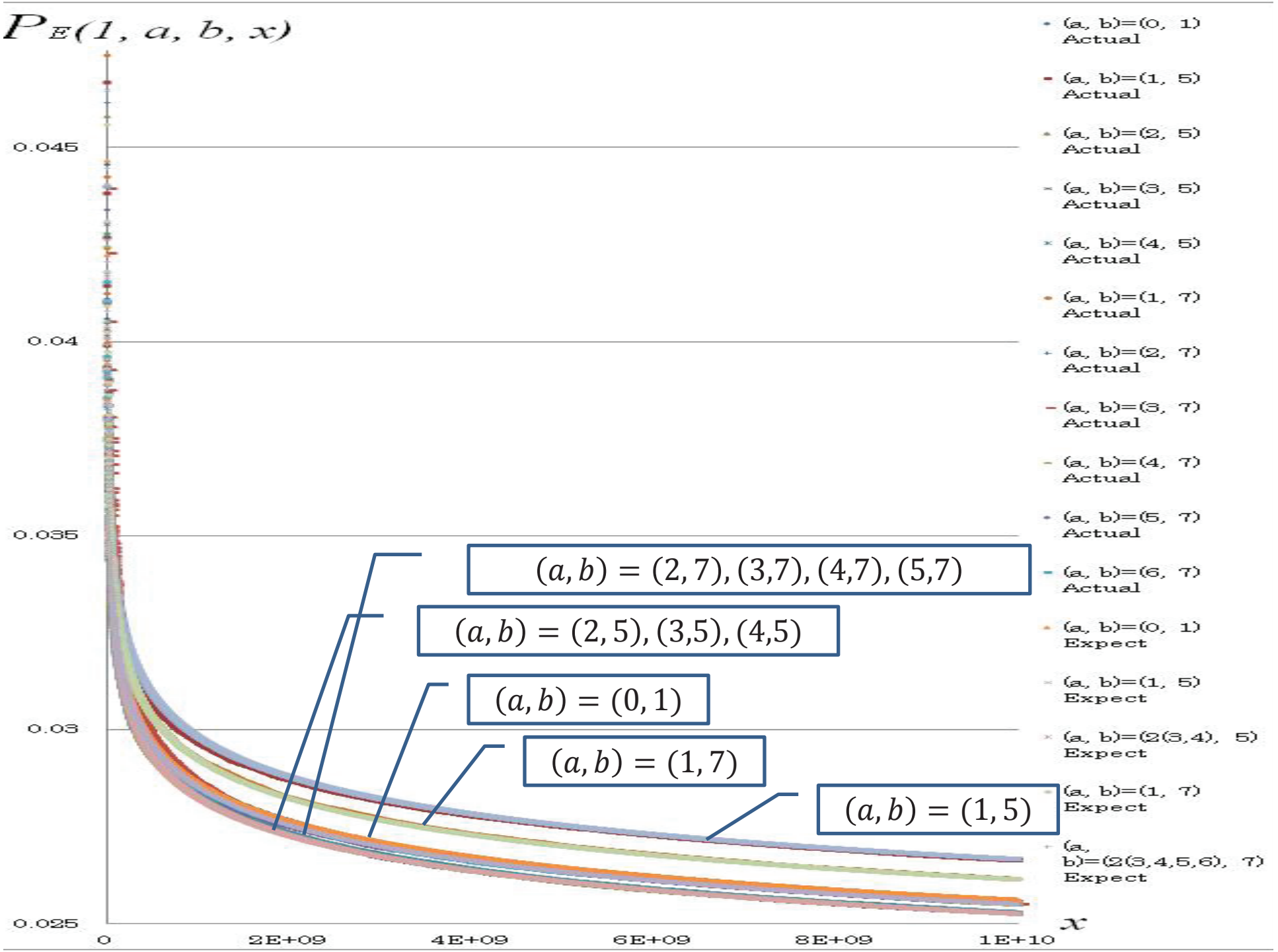
$E : y^2 = x^3 - 6x + 2, M = 6.$

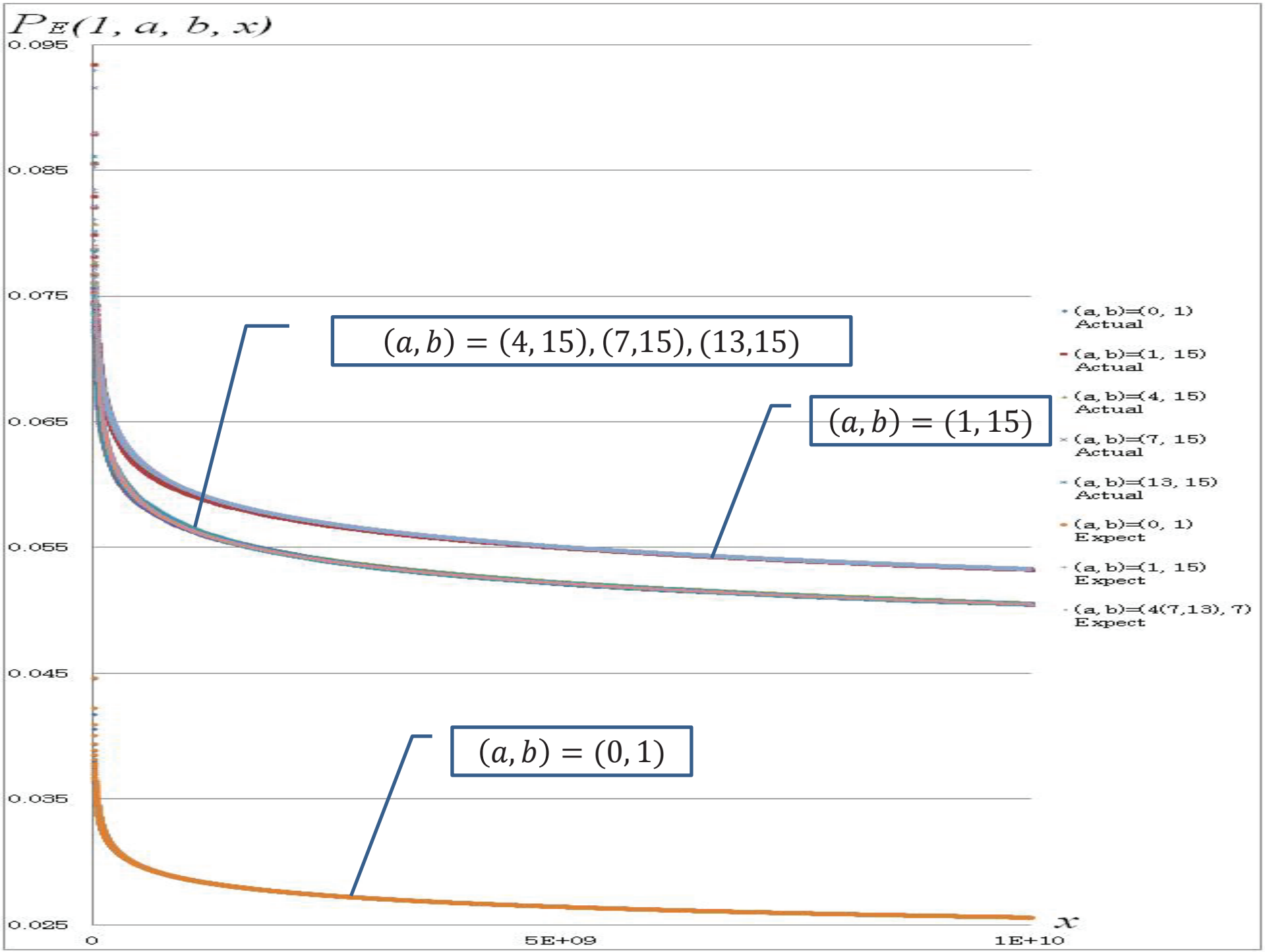
$C_{E,\,1}$ =0.561295742488261971297938 5….

$$C_{E,1,a,5} = \begin{cases} \frac{76}{73} & \text{if } a = 1 \\ \frac{72}{73} & \text{if } a \neq 1 \end{cases} \qquad C_{E,1,a,7} = \begin{cases} \frac{246}{241} & \text{if } a = 1 \\ \frac{240}{241} & \text{if } a \neq 1 \end{cases}$$

Moreover

$$C_{E,\,1,a,15} = \begin{cases} \frac{152}{73} & if\ a = 1 \\ \frac{144}{73} & if\ a = 4, 7, 13, \\ 0 & if\ a = 2, 8, 11, 14. \end{cases}$$


$P_E(1, a, b, x)$
0.045
0.04
0.035
0.03
0.025
0
2E+09
4E+09
6E+09
8E+09
1E+10
x
(a, b)=(0, 1) Actual
(a, b)=(1, 5) Actual
(a, b)=(2, 5) Actual
(a, b)=(3, 5) Actual
(a, b)=(4, 5) Actual
(a, b)=(1, 7) Actual
(a, b)=(2, 7) Actual
(a, b)=(3, 7) Actual
(a, b)=(4, 7) Actual
(a, b)=(5, 7) Actual
(a, b)=(6, 7) Actual
(a, b)=(0, 1) Expect
(a, b)=(1, 5) Expect
(a, b)=(2(3,4), 5) Expect
(a, b)=(1, 7) Expect
(a, b)=(2(3,4,5,6), 7) Expect
$(a, b) = (2, 7), (3, 7), (4, 7), (5, 7)$
$(a, b) = (2, 5), (3, 5), (4, 5)$
$(a, b) = (0, 1)$
$(a, b) = (1, 7)$
$(a, b) = (1, 5)$


$P_E(1, a, b, x)$
0.095
0.085
0.075
0.065
0.055
0.045
0.035
0.025
0
5E+09
1E+10
x
$(a, b) = (4, 15), (7,15), (13,15)$
$(a, b) = (1, 15)$
$(a, b) = (0, 1)$
(a, b)=(0, 1) Actual
(a, b)=(1, 15) Actual
(a, b)=(4, 15) Actual
(a, b)=(7, 15) Actual
(a, b)=(13, 15) Actual
(a, b)=(0, 1) Expect
(a, b)=(1, 15) Expect
(a, b)=(4(7,13), 7) Expect

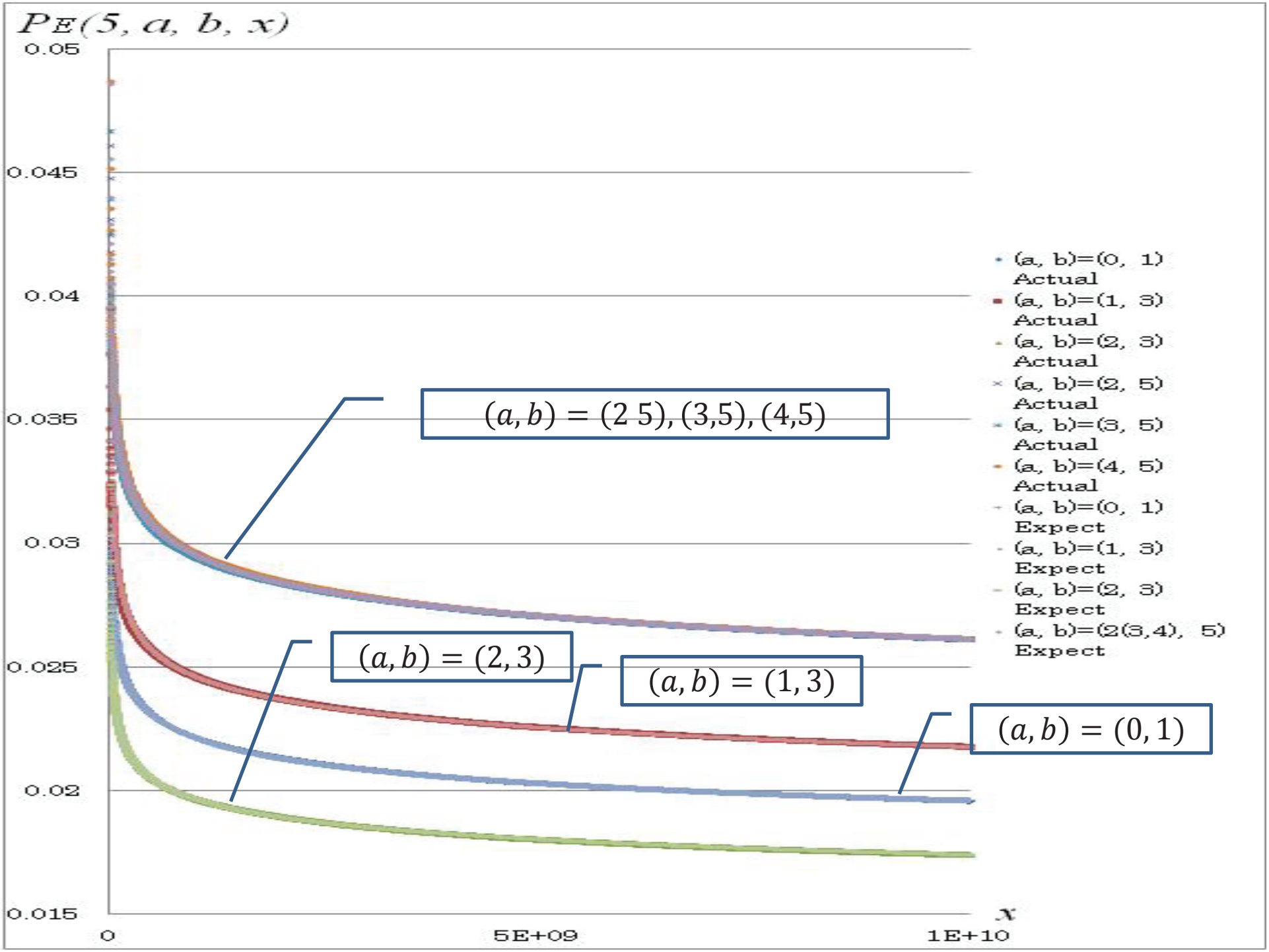
Example2 (Non-CM case)

$E: y^2 + y = x^3 - x^2 - 10x - 20, M = 2 \cdot 5 \cdot 11.$

$$C_{E,5,a,3} = \begin{cases} \frac{10}{9}, \\ \frac{8}{9}. \end{cases}$$

If $b = t = 5$, then $\gcd(b, Mt) = 5 \neq 1$. However, we can calculate $C_{E,5,a,5}$, because $G(2 \cdot 5^2 \cdot 11)$ is studied by Lang and Trotter, and so we know the structure of $G(2 \cdot 5^2 \cdot 11)$.

$$C_{E,5,a,5} = \begin{cases} 0 \; if \; a = 1, \\ \frac{4}{3} \; if \; a \neq 1. \end{cases}$$


$P_E(5, a, b, x)$
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0
5E+09
1E+10
x
(a, b)=(0, 1) Actual
(a, b)=(1, 3) Actual
(a, b)=(2, 3) Actual
(a, b)=(2, 5) Actual
(a, b)=(3, 5) Actual
(a, b)=(4, 5) Actual
(a, b)=(0, 1) Expect
(a, b)=(1, 3) Expect
(a, b)=(2, 3) Expect
(a, b)=(2(3,4), 5) Expect
$(a, b) = (2\ 5), (3,5), (4,5)$
$(a, b) = (2, 3)$
$(a, b) = (1, 3)$
$(a, b) = (0, 1)$

Example2 (CM case)

$E : y^2 = x^3 - x$, $M = 2, R = \mathbb{Z}[i], f_F = 4, f = 1.$

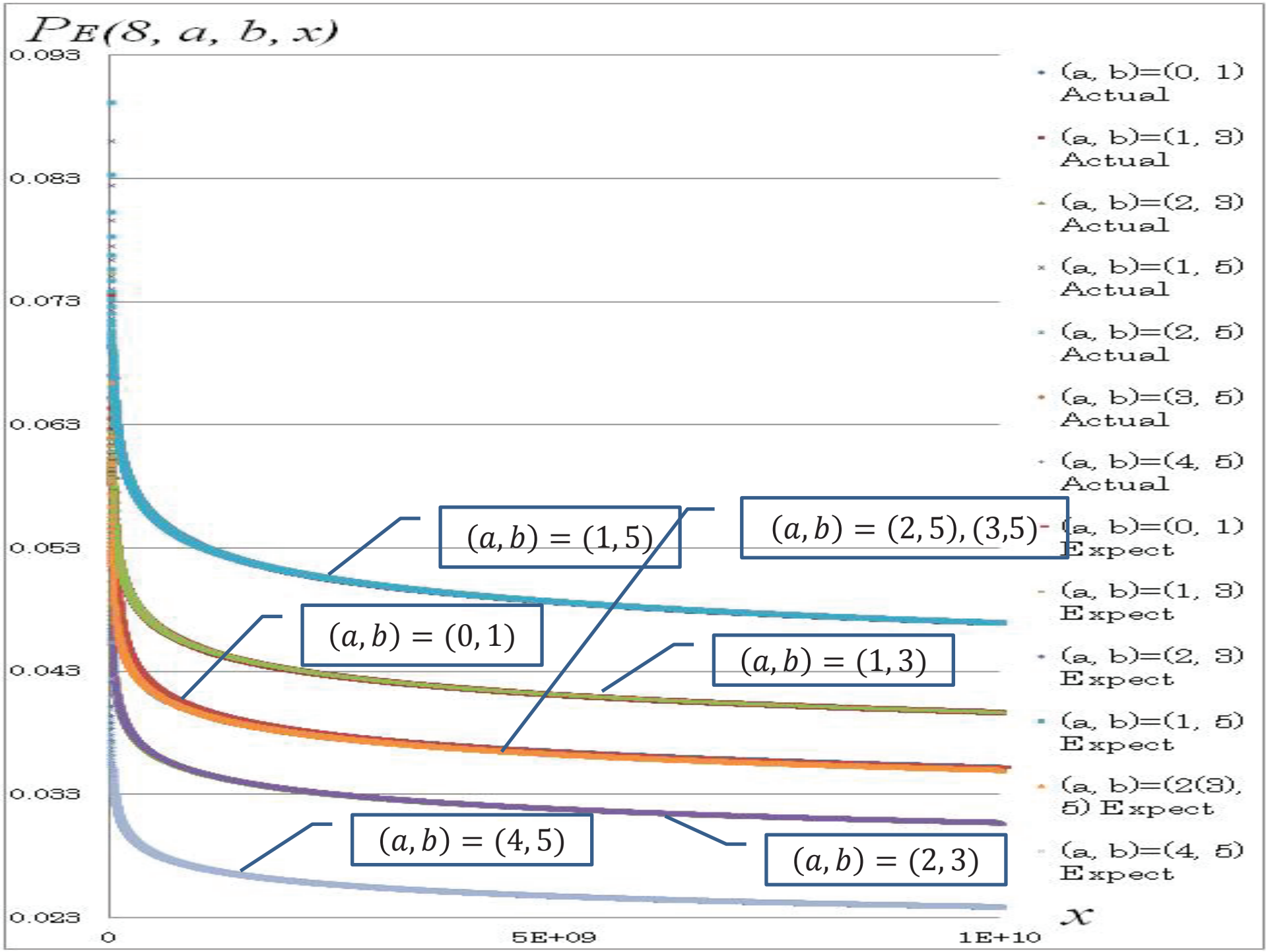
$C_{E,\,8} = 0.69871591214746\ldots$

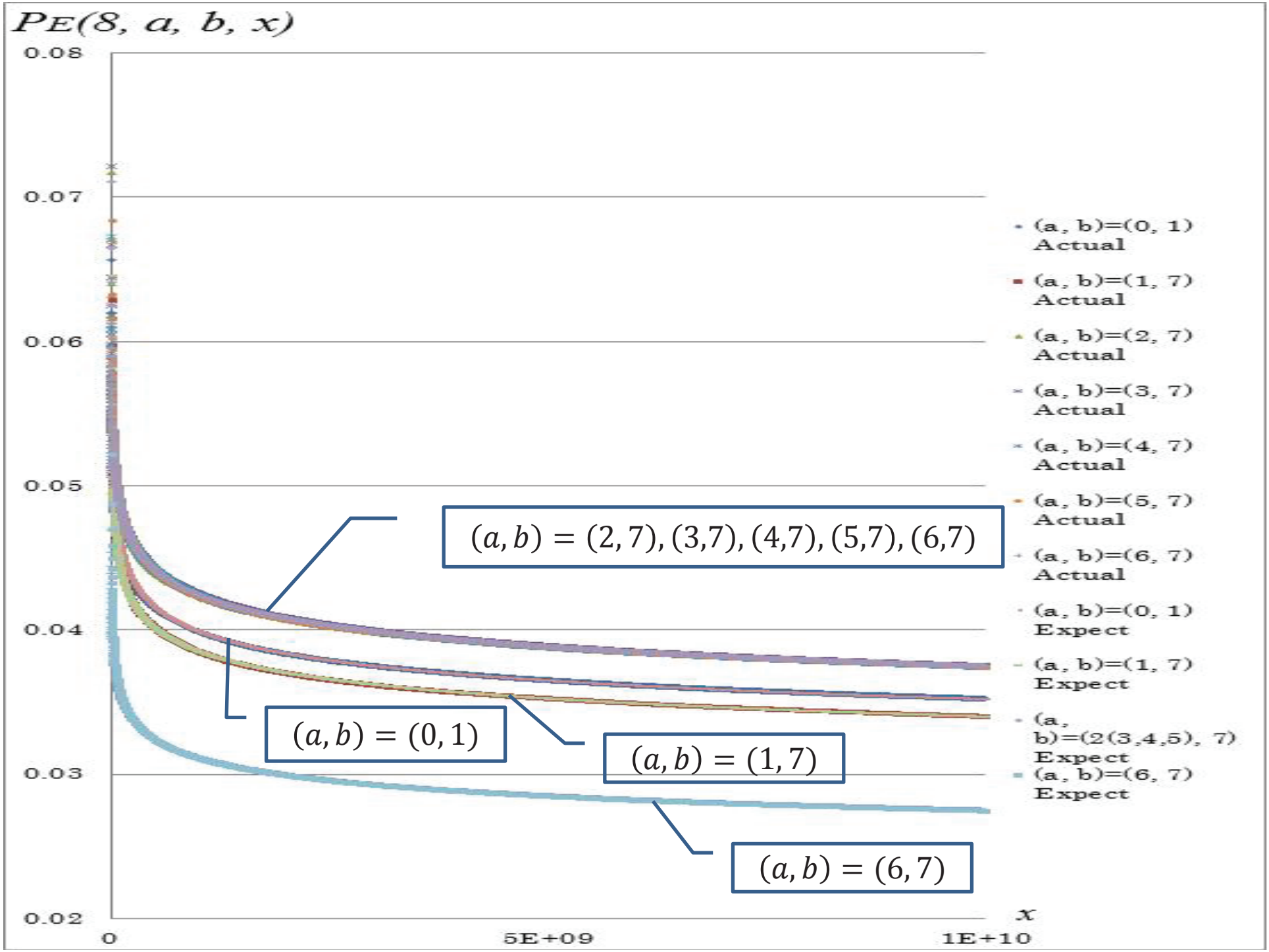
$C_{E_{\mathbb{Q}(i)},\,8} = 1.067350894\ldots$

$$C_{E,\,8,\,a,\,3} = \begin{cases} 1.127091875298942\ldots & \text{if } a = 1 \\ 0.872908124701058\ldots & \text{if } a \neq 1 \end{cases}$$

$$C_{E,\,8,\,a,\,5} = \begin{cases} 1.333333333333333\ldots & \text{if } a = 1 \\ 0.993869062616255\ldots & \text{if } a = 2,\ 3 \\ 0.678928541434156\ldots & \text{if } a = 4 \end{cases}$$

$$C_{E,\,8,\,a,\,7} = \begin{cases} 0.965986332526847\ldots & \text{if } a = 1 \\ 1.063492027307284\ldots & \text{if } a \neq 1,\ 6 \\ 0.780045558243498\ldots & \text{if } a = 6 \end{cases}$$


$P_E(8, a, b, x)$
0.093
0.083
0.073
0.063
0.053
0.043
0.033
0.023
0
5E+09
1E+10
x
(a, b)=(0, 1) Actual
(a, b)=(1, 3) Actual
(a, b)=(2, 3) Actual
(a, b)=(1, 5) Actual
(a, b)=(2, 5) Actual
(a, b)=(3, 5) Actual
(a, b)=(4, 5) Actual
(a, b)=(0, 1) Expect
(a, b)=(1, 3) Expect
(a, b)=(2, 3) Expect
(a, b)=(1, 5) Expect
(a, b)=(2(3), 5) Expect
(a, b)=(4, 5) Expect
$(a, b) = (1, 5)$
$(a, b) = (2, 5), (3, 5)$
$(a, b) = (0, 1)$
$(a, b) = (1, 3)$
$(a, b) = (4, 5)$
$(a, b) = (2, 3)$


PE(8, a, b, x)
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0
5E+09
1E+10
x
(a, b)=(0, 1) Actual
(a, b)=(1, 7) Actual
(a, b)=(2, 7) Actual
(a, b)=(3, 7) Actual
(a, b)=(4, 7) Actual
(a, b)=(5, 7) Actual
(a, b)=(6, 7) Actual
(a, b)=(0, 1) Expect
(a, b)=(1, 7) Expect
(a, b)=(2(3,4,5), 7) Expect
(a, b)=(6, 7) Expect
$(a,b) = (2,7), (3,7), (4,7), (5,7), (6,7)$
$(a,b) = (0,1)$
$(a,b) = (1,7)$
$(a,b) = (6,7)$

$P_E(1,0,1,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028640288	0.028637876	6000000000	0.026223783	0.026223329
2000000000	0.02766305	0.027652581	7000000000	0.026035527	0.026034675
3000000000	0.027102517	0.027107106	8000000000	0.025872841	0.025873494
4000000000	0.026729141	0.026733024	9000000000	0.025731157	0.025732895
5000000000	0.026445002	0.026450231	10000000000	0.025609361	0.025608326

$P_E(1,1,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.029683309	0.029814775	6000000000	0.027273820	0.027301000
2000000000	0.028712855	0.028788988	7000000000	0.027080172	0.027104593
3000000000	0.028161652	0.028221096	8000000000	0.026913190	0.026936789
4000000000	0.027783831	0.027831641	9000000000	0.026758016	0.026790411
5000000000	0.027502239	0.027537227	10000000000	0.026638621	0.026660723

$P_E(1,2,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028270462	0.028245577	6000000000	0.025856804	0.025864105
2000000000	0.027312707	0.027273778	7000000000	0.025679170	0.025678035
3000000000	0.026738474	0.026735776	8000000000	0.025513050	0.025519063
4000000000	0.026361056	0.026366818	9000000000	0.025377844	0.025380389
5000000000	0.026076024	0.026087899	10000000000	0.025256671	0.025257527

$P_E(1,3,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028324094	0.028245577	6000000000	0.025872954	0.025864105
2000000000	0.027296193	0.027273778	7000000000	0.025675933	0.025678035
3000000000	0.026725405	0.026735776	8000000000	0.025516022	0.025519063
4000000000	0.026364419	0.026366818	9000000000	0.025377178	0.025380389
5000000000	0.026086833	0.026087899	10000000000	0.025261585	0.025257527
$P_E(1,4,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028283343	0.028245577	6000000000	0.025891566	0.025864105
2000000000	0.027330484	0.027273778	7000000000	0.025706852	0.025678035
3000000000	0.026784579	0.026735776	8000000000	0.025549114	0.025519063
4000000000	0.026407275	0.026366818	9000000000	0.025411609	0.025380389
5000000000	0.026114931	0.026087899	10000000000	0.025280586	0.025257527
$P_E(1,1,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.029252010	0.029232023	6000000000	0.026787093	0.026767381
2000000000	0.028250240	0.028226286	7000000000	0.026589965	0.026574813
3000000000	0.027710793	0.027669494	8000000000	0.026419677	0.026410289
4000000000	0.027308621	0.027287651	9000000000	0.026278378	0.026266772
5000000000	0.027018229	0.026998991	10000000000	0.026149671	0.026139620

$P_E(1,2,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028456263	0.028519047	6000000000	0.026100654	0.026114518
2000000000	0.027528390	0.027537840	7000000000	0.025933627	0.025926647
3000000000	0.026969549	0.026994628	8000000000	0.025777114	0.025766136
4000000000	0.026611260	0.026622099	9000000000	0.025639945	0.025626119
5000000000	0.026327013	0.026340479	10000000000	0.025516608	0.025502068
$P_E(1,3,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028584957	0.028519047	6000000000	0.026095088	0.026114518
2000000000	0.027568842	0.027537840	7000000000	0.025904056	0.025926647
3000000000	0.026976858	0.026994628	8000000000	0.025752377	0.025766136
4000000000	0.026604671	0.026622099	9000000000	0.025617190	0.025626119
5000000000	0.026322474	0.026340479	10000000000	0.025495139	0.025502068
$P_E(1,4,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028549020	0.028519047	6000000000	0.026126800	0.026114518
2000000000	0.027557762	0.027537840	7000000000	0.025927402	0.025926647
3000000000	0.026993781	0.026994628	8000000000	0.025751858	0.025766136
4000000000	0.026631773	0.026622099	9000000000	0.025594890	0.025626119
5000000000	0.026350364	0.026340479	10000000000	0.025473708	0.025502068

$P_E(1,5,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028475697	0.028519047	6000000000	0.026108358	0.026114518
2000000000	0.027497563	0.027537840	7000000000	0.025918682	0.025926647
3000000000	0.026957687	0.026994628	8000000000	0.025758791	0.025766136
4000000000	0.026611717	0.026622099	9000000000	0.025617463	0.025626119
5000000000	0.026322551	0.026340479	10000000000	0.025505215	0.025502068
$P_E(1,6,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.028523700	0.028519047	6000000000	0.026124689	0.026114518
2000000000	0.027575445	0.027537840	7000000000	0.025939413	0.025926647
3000000000	0.027006404	0.026994628	8000000000	0.025777223	0.025766136
4000000000	0.026606784	0.026622099	9000000000	0.025639069	0.025626119
5000000000	0.026329372	0.026340479	10000000000	0.025515821	0.025502068

$P_E(1, 1, 15, x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.059371326	0.059629551	6000000000	0.054548205	0.054602000
2000000000	0.057429260	0.057577977	7000000000	0.054161053	0.054209186
3000000000	0.056326623	0.056442193	8000000000	0.053828214	0.053873578
4000000000	0.055568311	0.055663283	9000000000	0.053517706	0.053580823
5000000000	0.055004922	0.055074454	10000000000	0.053279207	0.053321447
$P_E(1, 4, 15, x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.056572735	0.056491154	6000000000	0.051786600	0.051728211
2000000000	0.054663939	0.054547557	7000000000	0.051415646	0.051356071
3000000000	0.053569945	0.053471552	8000000000	0.051100429	0.051038127
4000000000	0.052815552	0.052733637	9000000000	0.050824981	0.050760779
5000000000	0.052230967	0.052175798	10000000000	0.050561930	0.050515055
$P_E(1, 7, 15, x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.056538096	0.056491154	6000000000	0.051713658	0.051728211
2000000000	0.054626427	0.054547557	7000000000	0.051357763	0.051356071
3000000000	0.053477860	0.053471552	8000000000	0.051025443	0.051038127
4000000000	0.052724464	0.052733637	9000000000	0.050754605	0.050760779
5000000000	0.052151847	0.052175798	10000000000	0.050513846	0.050515055
$P_E(1, 13, 15, x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.056649856	0.056491154	6000000000	0.051746302	0.051728211
2000000000	0.054591432	0.054547557	7000000000	0.051351347	0.051356071
3000000000	0.053449776	0.053471552	8000000000	0.051031741	0.051038127
4000000000	0.052730033	0.052733637	9000000000	0.050754184	0.050760779
5000000000	0.052174477	0.052175798	10000000000	0.050522826	0.050515055

$P_E(5,0,1,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.022152893	0.022144232	6000000000	0.020123645	0.020123195
2000000000	0.021336450	0.021315702	7000000000	0.019966167	0.019966600
3000000000	0.020865162	0.020859291	8000000000	0.019831536	0.019832957
4000000000	0.020548077	0.020547216	9000000000	0.019712679	0.019716496
5000000000	0.020313097	0.020311776	10000000000	0.019610499	0.019613407
$P_E(5,1,3,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.024625027	0.024604703	6000000000	0.022374974	0.022359106
2000000000	0.023714458	0.023684114	7000000000	0.022196851	0.022185111
3000000000	0.023192720	0.023176990	8000000000	0.022046869	0.022036619
4000000000	0.022842760	0.022830240	9000000000	0.021914528	0.021907324
5000000000	0.022583294	0.022568641	10000000000	0.021800311	0.021792674
$P_E(5,2,3,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.019680966	0.019683762	6000000000	0.017872414	0.017887284
2000000000	0.018958583	0.018947291	7000000000	0.017735517	0.017748089
3000000000	0.018537686	0.018541592	8000000000	0.017616268	0.017629295
4000000000	0.018253506	0.018264192	9000000000	0.017510876	0.017525859
5000000000	0.018042947	0.018054912	10000000000	0.017420747	0.017434139

$P_E(5,2,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.029570302	0.029525643	6000000000	0.026822363	0.026830927
2000000000	0.028443894	0.028420937	7000000000	0.026613928	0.026622134
3000000000	0.027810500	0.027812388	8000000000	0.026434845	0.026443943
4000000000	0.027396045	0.027396288	9000000000	0.026272390	0.026288789
5000000000	0.027086294	0.027082369	10000000000	0.026140500	0.026151209
$P_E(5,3,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.029468792	0.029525643	6000000000	0.026820017	0.026830927
2000000000	0.028407614	0.028420937	7000000000	0.026609925	0.026622134
3000000000	0.027792564	0.027812388	8000000000	0.026435607	0.026443943
4000000000	0.027385584	0.027396288	9000000000	0.026280147	0.026288789
5000000000	0.027072018	0.027082369	10000000000	0.026148759	0.026151209
$P_E(5,4,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.029571249	0.029525643	6000000000	0.026851941	0.026830927
2000000000	0.028493465	0.028420937	7000000000	0.026640448	0.026622134
3000000000	0.027856753	0.027812388	8000000000	0.026455438	0.026443943
4000000000	0.027410332	0.027396288	9000000000	0.026297808	0.024048390
5000000000	0.027093743	0.027082369	10000000000	0.026152358	0.026151209

$P_E(8,0,1,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.039884962	0.039901509	6000000000	0.036156835	0.036169783
2000000000	0.038335953	0.038369372	7000000000	0.035873168	0.035881428
3000000000	0.037504973	0.037526748	8000000000	0.035631045	0.035635425
4000000000	0.036942546	0.036951143	9000000000	0.035417906	0.035421119
5000000000	0.036505217	0.036517181	10000000000	0.035228442	0.035231475
$P_E(8,1,3,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.044926912	0.044972693	6000000000	0.040741296	0.040766692
2000000000	0.043197532	0.043245833	7000000000	0.040431756	0.040441690
3000000000	0.042270214	0.042296118	8000000000	0.040155806	0.040164422
4000000000	0.041631397	0.041647358	9000000000	0.039916747	0.039922879
5000000000	0.041130211	0.041158243	10000000000	0.039706359	0.039709133
$P_E(8,2,3,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.034843433	0.034830324	6000000000	0.031572572	0.031572873
2000000000	0.033474660	0.033492911	7000000000	0.031314647	0.031321166
3000000000	0.032739902	0.032757378	8000000000	0.031106416	0.031106428
4000000000	0.032253925	0.032254928	9000000000	0.030919158	0.030919359
5000000000	0.031880318	0.031876120	10000000000	0.030750647	0.030753817

$P_E(8,1,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.053228105	0.053202012	6000000000	0.048187255	0.048226377
2000000000	0.051117679	0.051159163	7000000000	0.047804421	0.047841904
3000000000	0.049988729	0.050035664	8000000000	0.047485954	0.047513900
4000000000	0.049247980	0.049268191	9000000000	0.047206575	0.047228159
5000000000	0.048660480	0.048689575	10000000000	0.046958101	0.046975300
$P_E(8,2,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.039639518	0.039656885	6000000000	0.035965264	0.035948037
2000000000	0.038140378	0.038134142	7000000000	0.035681467	0.035661451
3000000000	0.037312561	0.037296684	8000000000	0.035434204	0.035416955
4000000000	0.036741499	0.036724607	9000000000	0.035218889	0.035203964
5000000000	0.036303592	0.036293306	10000000000	0.035024653	0.035015482
$P_E(8,3,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.039589226	0.039656885	6000000000	0.035937525	0.035948037
2000000000	0.038072943	0.038134142	7000000000	0.035660325	0.035661451
3000000000	0.037264892	0.037296684	8000000000	0.035422442	0.035416955
4000000000	0.036709427	0.036724607	9000000000	0.035207751	0.035203964
5000000000	0.036279298	0.036293306	10000000000	0.035021167	0.035015482

$P_E(8,4,5,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.027082997	0.027090252	6000000000	0.024537393	0.024556679
2000000000	0.026013325	0.026050042	7000000000	0.024346385	0.024360907
3000000000	0.025453846	0.025477961	8000000000	0.024181455	0.024193888
4000000000	0.025071023	0.025087166	9000000000	0.024038474	0.024048390
5000000000	0.024777438	0.024792537	10000000000	0.023909839	0.023919635
$P_E(8,1,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.038511268	0.038544281	6000000000	0.034934617	0.034939484
2000000000	0.037015808	0.037064253	7000000000	0.034664333	0.034660938
3000000000	0.036208409	0.036250292	8000000000	0.034437906	0.034423303
4000000000	0.035673026	0.035694272	9000000000	0.034218907	0.034216287
5000000000	0.035274622	0.035275065	10000000000	0.034035654	0.034033094
$P_E(8,2,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.042393945	0.042434902	6000000000	0.038449736	0.038466240
2000000000	0.040747490	0.040805482	7000000000	0.038140537	0.038159578
3000000000	0.039896884	0.039909360	8000000000	0.037885271	0.037897957
4000000000	0.039283803	0.039297216	9000000000	0.037669209	0.037670045
5000000000	0.038806989	0.038835695	10000000000	0.037471394	0.037468360

$P_E(8,3,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.042489766	0.042434902	6000000000	0.038496922	0.038466240
2000000000	0.040839043	0.040805482	7000000000	0.038195669	0.038159578
3000000000	0.039951119	0.039909360	8000000000	0.037929754	0.037897957
4000000000	0.039342174	0.039297216	9000000000	0.037699978	0.037670045
5000000000	0.038875829	0.038835695	10000000000	0.037491219	0.037468360
$P_E(8,4,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.042397935	0.042434902	6000000000	0.038413016	0.038466240
2000000000	0.040741634	0.040805482	7000000000	0.038121209	0.038159578
3000000000	0.039846378	0.039909360	8000000000	0.037862492	0.037897957
4000000000	0.039254684	0.039297216	9000000000	0.037634084	0.037670045
5000000000	0.038782045	0.038835695	10000000000	0.037433426	0.037468360
$P_E(8,5,7,x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.042359961	0.042434902	6000000000	0.038440622	0.038466240
2000000000	0.040723283	0.040805482	7000000000	0.038138995	0.038159578
3000000000	0.039860842	0.039909360	8000000000	0.037878964	0.037897957
4000000000	0.039284406	0.039297216	9000000000	0.037656674	0.037670045
5000000000	0.038812677	0.038835695	10000000000	0.037456653	0.037468360

$P_E(8, 6, 7, x)$					
x	Actual	Expected	x	Actual	Expected
1000000000	0.031156936	0.031124970	6000000000	0.028206078	0.028214052
2000000000	0.029948498	0.029929829	7000000000	0.027978517	0.027989123
3000000000	0.029266142	0.029272545	8000000000	0.027792170	0.027797230
4000000000	0.028817381	0.028823553	9000000000	0.027628804	0.027630062
5000000000	0.028479174	0.028485038	10000000000	0.027482336	0.027482132