Random Involutions and the Distinct Prime Divisor Function

Zubin Mukerjee and Uthsav Chitra
Advisor: Kirsten Wickelgren, Harvard University
PROMYS 2012

Albany Area Math Circle

April 6, 2013

DISTINCT PRIME DIVISOR FUNCTION

- Any positive integer n factors uniquely as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_d^{e_d}$$

where $p_1, p_2, p_3, ..., p_d$ are distinct prime numbers. Let $d(n)$ be the number of distinct prime factors of n.

DISTINCT PRIME DIVISOR FUNCTION

- Any positive integer n factors uniquely as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_d^{e_d}$$

  where $p_1, p_2, p_3, ..., p_d$ are distinct prime numbers. Let $d(n)$ be the number of distinct prime factors of n.

- $d(9) = 1$

Distinct Prime Divisor Function

- Any positive integer n factors uniquely as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_d^{e_d}$$

  where $p_1, p_2, p_3, ..., p_d$ are distinct prime numbers. Let $d(n)$ be the number of distinct prime factors of n.
- $d(9) = 1$
- $d(6) = 2$

DISTINCT PRIME DIVISOR FUNCTION

- Any positive integer n factors uniquely as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_d^{e_d}$$

  where $p_1, p_2, p_3, ..., p_d$ are distinct prime numbers. Let $d(n)$ be the number of distinct prime factors of n.
- $d(9) = 1$
- $d(6) = 2$
- Our goal in our project was to determine whether a specific relationship could be used to approximate $\sum_{n=N+1}^{M} d(n)$ (for arbitrary integers M and N).

DEFINITIONS

- Let $\mathbb{F}_2$ denote the field with 2 elements, so $\mathbb{F}_2 = \mathbb{Z}/2$.

DEFINITIONS

- Let $\mathbb{F}_2$ denote the field with 2 elements, so $\mathbb{F}_2 = \mathbb{Z}/2$.
- For each n, there exists a *modular curve* $X_0(n)$ with *genus* $g(n)$.

Definitions

- Let $\mathbb{F}_2$ denote the field with 2 elements, so $\mathbb{F}_2 = \mathbb{Z}/2$.
- For each n, there exists a *modular curve* $X_0(n)$ with *genus* $g(n)$.
- An *involution* is a map f such that composing f with itself gives the identity map

$$ff = id$$

DEFINITIONS

- Let $\mathbb{F}_2$ denote the field with 2 elements, so $\mathbb{F}_2 = \mathbb{Z}/2$.
- For each n, there exists a *modular curve* $X_0(n)$ with *genus* $g(n)$.
- An *involution* is a map f such that composing f with itself gives the identity map

$$ff = id$$

Definitions

- From $X_0(n)$ one can obtain (up to isomorphism) an involution $\tau(n)$ on $\mathbb{F}_2^{2g(n)}$.

DEFINITIONS

- From $X_0(n)$ one can obtain (up to isomorphism) an involution $\tau(n)$ on $\mathbb{F}_2^{2g(n)}$.
- It is known that for n odd, there are exactly

$$2^{g(n)+2^{d-1}-1}$$

elements of $\mathbb{F}_2^{2g(n)}$ which are fixed by this involution $\tau(n)$.

DEFINITIONS

- From $X_0(n)$ one can obtain (up to isomorphism) an involution $\tau(n)$ on $\mathbb{F}_2^{2g(n)}$.
- It is known that for n odd, there are exactly

$$2^{g(n)+2^{d-1}-1}$$

elements of $\mathbb{F}_2^{2g(n)}$ which are fixed by this involution $\tau(n)$.
- $d(n)$ is determined by the involution $\tau(n)$ and the genus $g(n)$.

Definitions

- From $X_0(n)$ one can obtain (up to isomorphism) an involution $\tau(n)$ on $\mathbb{F}_2^{2g(n)}$.
- It is known that for n odd, there are exactly

$$2^{g(n)+2^{d-1}-1}$$

  elements of $\mathbb{F}_2^{2g(n)}$ which are fixed by this involution $\tau(n)$.
- $d(n)$ is determined by the involution $\tau(n)$ and the genus $g(n)$.
- Can we model the number of prime factors of an integer by a random involution?

NUMBER OF FINITE SETS

- It is often useful to count objects X, weighted by $\frac{1}{|\operatorname{Aut}(X)|}$, where $\operatorname{Aut}(X)$ denotes the group of automorphisms of X (isomorphisms from X to itself).

Number of Finite Sets

- It is often useful to count objects X, weighted by $\frac{1}{|\operatorname{Aut}(X)|}$, where $\operatorname{Aut}(X)$ denotes the group of automorphisms of X (isomorphisms from X to itself).
- Every nonempty finite set is in bijection with a set of the form $\{1, 2, \ldots, n\}$, so up to isomorphism, the finite sets are $\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots$

NUMBER OF FINITE SETS

- It is often useful to count objects X, weighted by $\frac{1}{|\operatorname{Aut}(X)|}$, where $\operatorname{Aut}(X)$ denotes the group of automorphisms of X (isomorphisms from X to itself).
- Every nonempty finite set is in bijection with a set of the form $\{1, 2, \ldots, n\}$, so up to isomorphism, the finite sets are $\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, ...$
- For a finite set with k elements, the number of automorphisms is precisely the number of permutations of k elements: $k! = (k)(k-1)...(2)(1)$

NUMBER OF FINITE SETS

- It is often useful to count objects X, weighted by $\frac{1}{|\operatorname{Aut}(X)|}$, where $\operatorname{Aut}(X)$ denotes the group of automorphisms of X (isomorphisms from X to itself).
- Every nonempty finite set is in bijection with a set of the form $\{1, 2, \ldots, n\}$, so up to isomorphism, the finite sets are $\emptyset, \{1\}, \{1,2\}, \{1,2,3\}, ...$
- For a finite set with k elements, the number of automorphisms is precisely the number of permutations of k elements: $k! = (k)(k-1)...(2)(1)$
- Thus, the 'number' of random finite sets is $\sum_{k=0}^{\infty} \frac{1}{k!} = e$.

$\mathbb{F}_2^m$ VECTOR SPACES

- For any positive integer m, $\mathbb{F}_2^m$ has the structure of an $\mathbb{F}_2$-**vector space**.

$\mathbb{F}_2^m$ VECTOR SPACES

- For any positive integer m, $\mathbb{F}_2^m$ has the structure of an $\mathbb{F}_2$-**vector space**.
- The converse is also true: any $\mathbb{F}_2$-vector space is isomorphic to $\mathbb{F}_2^m$ for a positive integer m.

Automorphisms of $\mathbb{F}_2^m$

- The automorphisms of $\mathbb{F}_2^m$ are the elements of $GL_m\,\mathbb{F}_2$, or the group of m x m invertible matrices.

AUTOMORPHISMS OF $\mathbb{F}_2^{\mathrm{m}}$

- The automorphisms of $\mathbb{F}_2^{\mathrm{m}}$ are the elements of $\mathrm{GL_m}\,\mathbb{F}_2$, or the group of m x m invertible matrices.
- $$|\,\mathrm{GL_m}\,\mathbb{F}_2| = \prod_{n=1}^{m}(2^m - 2^{n-1})$$

AUTOMORPHISMS OF $\mathbb{F}_2^m$

- The automorphisms of $\mathbb{F}_2^m$ are the elements of $\mathrm{GL}_m\,\mathbb{F}_2$, or the group of m x m invertible matrices.
- $$|\mathrm{GL}_m\,\mathbb{F}_2| = \prod_{n=1}^{m}(2^m - 2^{n-1})$$
- Thus, the number of $\mathbb{F}_2$-vector spaces of dimension m is equal to
$$\sum_{m=1}^{\infty}\prod_{n=1}^{m}\frac{1}{2^m - 2^{n-1}}$$

$\mathbb{F}_2[\mathbb{Z}/2]$ modules

- An $\mathbb{F}_2$-vector space with involution is equivalent to a module over the ring $\mathbb{F}_2[\mathbb{Z}/2]$.
- This identification is useful in determining the number of automorphisms of $\mathbb{F}_2$-vector spaces with involution.

$\mathbb{F}_2[\mathbb{Z}/2]$-MODULES

- Since the involution f is acting on $\mathbb{F}_2^m$, it will be in the form of an $m \times m$ matrix.

$\mathbb{F}_2[\mathbb{Z}/2]$-modules

- Since the involution f is acting on $\mathbb{F}_2^m$, it will be in the form of an $m \times m$ matrix.

Theorem

Any $\mathbb{F}_2[\mathbb{Z}/2]$-module is isomorphic to $\mathbb{F}_2[\mathbb{Z}/2]^a$ x $\mathbb{F}_2^b$ for a unique pair of non-negative integers (a, b).

$\mathbb{F}_2[\mathbb{Z}/2]$-modules

- Since the involution f is acting on $\mathbb{F}_2^m$, it will be in the form of an $m \times m$ matrix.

Theorem

Any $\mathbb{F}_2[\mathbb{Z}/2]$-module is isomorphic to $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}}$ x $\mathbb{F}_2^{\mathrm{b}}$ for a unique pair of non-negative integers (a, b).

- (Serge Lang's *Algebra*, Ch. 3, Sec. 7)

$\mathbb{F}_2[\mathbb{Z}/2]$-MODULES

- Since the involution f is acting on $\mathbb{F}_2^m$, it will be in the form of an $m \times m$ matrix.

Theorem

Any $\mathbb{F}_2[\mathbb{Z}/2]$-module is isomorphic to $\mathbb{F}_2[\mathbb{Z}/2]^a$ x $\mathbb{F}_2^b$ for a unique pair of non-negative integers (a, b).

- (Serge Lang's *Algebra*, Ch. 3, Sec. 7)

$\mathbb{F}_2[\mathbb{Z}/2]$-MODULES

- In general, the $\mathbb{F}_2[\mathbb{Z}/2]$-module $\mathbb{F}_2[\mathbb{Z}/2]^a \times \mathbb{F}_2^b$ corresponds to the $\mathbb{F}_2$-vector space $\mathbb{F}_2^{2a+b}$ together with an involution f whose $(2a+b) \times (2a+b)$ matrix is given by:

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{0} & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \mathbf{0} & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & \mathbf{1} & \mathbf{0} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \mathbf{1} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix}$$

(where there are a copies of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ matrices diagonally for the upper left $2a \times 2a$ corner of the matrix, followed by b copies of 1's along the diagonal for the bottom right $b \times b$ corner).

Fixed points in a $\mathbb{F}_2$-vector space

- In $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}} \times \mathbb{F}_2^{\mathrm{b}}$ there are $(2^a)(2^b) = 2^{a+b}$ fixed points.
- Recall that the involution $\tau(n)$ on $\mathbb{F}_2^{2g(n)}$ has exactly $2^{g(n)+2^{d-1}-1}$ fixed points.

FIXED POINTS IN A $\mathbb{F}_2$-VECTOR SPACE

- In $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}}$ x $\mathbb{F}_2^{\mathrm{b}}$ there are $(2^a)(2^b) = 2^{a+b}$ fixed points.
- Recall that the involution $\tau(n)$ on $\mathbb{F}_2^{2g(n)}$ has exactly $2^{g(n)+2^{d-1}-1}$ fixed points.

$$a + b = g(n) + 2^{d-1} - 1$$
$$2a + b = 2g(n)$$

FIXED POINTS IN A $\mathbb{F}_2$-VECTOR SPACE

- In $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}}$ x $\mathbb{F}_2^{\mathrm{b}}$ there are $(2^a)(2^b) = 2^{a+b}$ fixed points.
- Recall that the involution $\tau(n)$ on $\mathbb{F}_2^{2g(n)}$ has exactly $2^{g(n)+2^{d-1}-1}$ fixed points.

$$a + b = g(n) + 2^{d-1} - 1$$
$$2a + b = 2g(n)$$

- Solving this system yields

$$a = g(n) - 2^{d-1} + 1$$

and

$$b = 2(2^{d-1} - 1)$$

FIXED POINTS IN A $\mathbb{F}_2$-VECTOR SPACE

- In $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}} \times \mathbb{F}_2^{\mathrm{b}}$ there are $(2^a)(2^b) = 2^{a+b}$ fixed points.
- Recall that the involution $\tau(n)$ on $\mathbb{F}_2^{2g(n)}$ has exactly $2^{g(n)+2^{d-1}-1}$ fixed points.

$$a + b = g(n) + 2^{d-1} - 1$$
$$2a + b = 2g(n)$$

- Solving this system yields

$$a = g(n) - 2^{d-1} + 1$$

and

$$b = 2(2^{d-1} - 1)$$

- Rearranged:

$$d = \log_2 (g - a + 1)$$

AUTOMORPHISMS OF $\mathbb{F}_2[\mathbb{Z}/2]^a$ x $\mathbb{F}_2^b$

Theorem

Let (a, b) be a pair of non-negative integers. The number of automorphisms of the $\mathbb{F}_2[\mathbb{Z}/2]$-module $\mathbb{F}_2[\mathbb{Z}/2]^a$ x $\mathbb{F}_2^b$ is exactly

$$|\operatorname{GL}_a \mathbb{F}_2||\operatorname{GL}_b \mathbb{F}_2||\operatorname{Mat}_{bxa} \mathbb{F}_2|^2|\operatorname{Mat}_{axa} \mathbb{F}_2|.$$

AUTOMORPHISMS OF $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}}$ X $\mathbb{F}_2^{\mathrm{b}}$

Theorem

Let (a, b) be a pair of non-negative integers. The number of automorphisms of the $\mathbb{F}_2[\mathbb{Z}/2]$-module $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}}$ x $\mathbb{F}_2^{\mathrm{b}}$ is exactly

$$|\operatorname{GL}_{\mathrm{a}} \mathbb{F}_2||\operatorname{GL}_{\mathrm{b}} \mathbb{F}_2||\operatorname{Mat}_{\mathrm{bxa}} \mathbb{F}_2|^2|\operatorname{Mat}_{\mathrm{axa}} \mathbb{F}_2|.$$

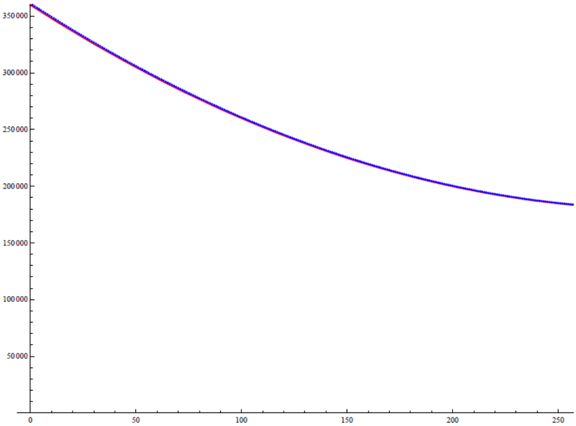
- Using the expressions for $|\operatorname{GL}_m \mathbb{F}_2|$ that we developed earlier, we can simplify the automorphism equation to the following:

$$|\mathrm{Aut}(a, b)| = \left(\prod_{x=1}^{a}(2^a - 2^{x-1})\right)\left(\prod_{y=1}^{b}(2^b - 2^{y-1})\right)(2^{ab})^2(2^{a^2})$$

Automorphisms of $\mathbb{F}_2[\mathbb{Z}/2]^a \times \mathbb{F}_2^b$

- $$|\mathrm{Aut}(a,b)| \approx C \cdot 2^{a^2+(a+b)^2}$$

  for a certain constant C.



COUNTING AND PROBABILITIES WITH $\mathbb{F}_2$-VECTOR SPACES

- Given a natural number n and a pair (a, b) of non-negative integers such that $2a + b = n$, the probability that an involution on $\mathbb{F}_2^{\mathrm{n}}$ is isomorphic to the involution corresponding to $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}}$ x $\mathbb{F}_2^{\mathrm{b}}$ is:

$$\frac{1/|\operatorname{Aut}(a,b)|}{\sum_{a',b'}(1/|\operatorname{Aut}(a,b)|)} = \frac{\frac{1}{2^{a^2+(a+b)^2}}}{\sum_{a=0}^{\lfloor\frac{n}{2}\rfloor}\frac{1}{2^{a^2+(a+(n-2a))^2}}}$$

  where the sum is taken over all pairs of non-negative integers (a', b') such that $2a' + b' = n$.

COUNTING AND PROBABILITIES WITH $\mathbb{F}_2$-VECTOR SPACES

- For $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}}$ x $\mathbb{F}_2^{\mathrm{b}}$, the number of fixed points is 2^{a+b}. Therefore, the expected number of fixed points of an involution on $\mathbb{F}_2$ is:

$$\sum_{a',b'} f(a',b') \cdot 2^{a+b}$$

where $f(a,b)$ is fraction from the previous slide which represents the probability of an involution on $\mathbb{F}_2^{\mathrm{n}}$ being isomorphic to $\mathbb{F}_2[\mathbb{Z}/2]^{\mathrm{a}}$ x $\mathbb{F}_2^{\mathrm{b}}$, and the sum is being taken over all (a',b') such that $2a'+b'=n$.

COUNTING AND PROBABILITIES WITH $\mathbb{F}_2$-VECTOR SPACES

- The total number of $\mathbb{F}_2$-vector spaces with involution is given by the sum

$$\sum_{n=1}^{\infty} \sum_{a',b'} \frac{1}{\mathrm{Aut}(a',b')} = \sum_{n=1}^{\infty} \sum_{a=0}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{\mathrm{Aut}(a,n-2a)}$$

COUNTING AND PROBABILITIES WITH $\mathbb{F}_2$-VECTOR SPACES

- The total number of $\mathbb{F}_2$-vector spaces with involution is given by the sum

$$\sum_{n=1}^{\infty} \sum_{a',b'} \frac{1}{\mathrm{Aut}(a',b')} = \sum_{n=1}^{\infty} \sum_{a=0}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{\mathrm{Aut}(a,n-2a)}$$

- Let the above sum be D. Then the probability that a randomly chosen $\mathbb{F}_2$-vector space with involution will have dimension n is

$$\frac{\sum_{a',b'} \frac{1}{\mathrm{Aut}(a',b')}}{\sum_{n=1}^{\infty} \sum_{a=0}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{\mathrm{Aut}(a,n-2a)}} = \frac{\sum_{a=0}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{\mathrm{Aut}(a,n-2a)}}{\sum_{n=1}^{\infty} \sum_{a=0}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{\mathrm{Aut}(a,n-2a)}}$$

Random Involutions and $\tau(n)$

- Goal: compare random involutions with $\tau(n)$ (and thereby the approximations for $d(n)$) for odd values of n.

RANDOM INVOLUTIONS AND $\tau(n)$

- Goal: compare random involutions with $\tau(n)$ (and thereby the approximations for $d(n)$) for odd values of n.
- Computing the expected value of $d(n)$ using the involution $\tau(n)$ gives the following formula:

$$\frac{\displaystyle\sum_{a=1}^{g(n)} \frac{\log_2 (g(n) - a + 1)}{\text{Aut}(a, 2g(n) - a)}}{\displaystyle\sum_{n=1}^{g(n)} \frac{1}{\text{Aut}(a, 2g(n) - a)}}$$

RANDOM INVOLUTIONS AND $\tau(n)$

- Goal: compare random involutions with $\tau(n)$ (and thereby the approximations for $d(n)$) for odd values of n.
- Computing the expected value of $d(n)$ using the involution $\tau(n)$ gives the following formula:

$$\frac{\displaystyle\sum_{a=1}^{g(n)} \frac{\log_2\left(g(n)-a+1\right)}{\mathrm{Aut}(a, 2g(n)-a)}}{\displaystyle\sum_{n=1}^{g(n)} \frac{1}{\mathrm{Aut}(a, 2g(n)-a)}}$$

- Analysis with Mathematica suggests that this value tends to a constant.

Works Cited/Acknowledgements

- Thanks to the Program in Mathematics for Young Scientists (PROMYS) and the Clay Mathematics Institute.

Works Cited/Acknowledgements

- Thanks to the Program in Mathematics for Young Scientists (PROMYS) and the Clay Mathematics Institute.
- Lang, Serge. *Algebra*, third ed. Graduate Texts in Mathematics, vol. 211, Springer-Verlag. New York, 2002.

Works Cited/Acknowledgements

- Thanks to the Program in Mathematics for Young Scientists (PROMYS) and the Clay Mathematics Institute.

- Lang, Serge. *Algebra*, third ed. Graduate Texts in Mathematics, vol. 211, Springer-Verlag. New York, 2002.
- A full bibliography is available from the authors upon request.