

המחלקה למתמטיקה, בן-גוריון

---

---

## אשנב למתמטיקה

---

---

ביום שלישי, 5 במרץ, 2019

בשעה 18:15 – 19:45

באולם 101-

ההרצאה

### לפרק לגורמים את האלגוריתם של שור

תינתן על-ידי

שי (דשא) ויבורסקי

**תקציר:** לפרק מספר ממש גדול לגורמים ראשוניים זה קל. כל מה שצריך זה קצת זמן, קצת סבלנות, ומחשב קוונטי.

בשנת 1994 פיטר שור הראה איך אפשר לפרק מספרים לגורמים ראשוניים בזמן פולינומיאלי בעזרת מחשב קוונטי ובכך קידם את המעמד של המחשבים הקוונטיים מקוריוז משעשע למוקד מחקר ענף.

בהרצאה נסביר (מתמטית) מה הוא מחשב קוונטי, מה הוא יכול ולא יכול לעשות, ואיך נשתמש במחשב כזה בשביל לפרק מספרים לגורמים ראשוניים. אם הזמן יתיר, נדון בחשיבות התאורטית של התוצאה הזאת וקצת בתחום באופן כללי

**אנא שימו לב לשינוי בשעה!**