נימוקי ועדת פרס Erdos להענקת הפרס לפרופ' נתן קלר

נתן קלר הינו חוקר בעל שם עולמי שלזכותו הישגים פורצי דרך בשני תחומים מתמטיים מרכזיים, אשר במידה רבה אינם תלויים זה בזה: האחד הינו אנליזת פורייה דיסקרטית ושימושיה הקומבינטוריים, והשני הינו קריפטוגרפיה מודרנית עם דגש על פתוח שיטות תקיפה מעשיות של צפנים בעלי מפתח סימטרי.

בצד הקומבינטורי של עבודתו, נתן ושותפיו למחקר (ביניהם תלמידו נועם ליפשיץ, ו- David Ellis מלונדון), שכללו ופתחו כלים מאנליזה הרמונית מעל הקובייה הדיסקרטית, ובעזרתם יישבו (לתחום נרחב של פרמטרים) שורה של בעיות פתוחות מפורסמות בתורת הקבוצות הסופיות, ביניהן: השערת Erdos-Sos על הגודל המרבי של k-היפרגרף שאינו מכיל חיתוכים בגודל קבוע, השערת הסימפלקס המיוחד של Frankl-Furedi, והשערת Erdos-Chvatal על היפרגרפים בעלי עצב (nerve) שאינו מכיל שפה של d-סימפלקס. בכוון אחר, נתן השתמש באנליזת פורייה כדי להוכיח גרסאות כמותיות אופטימליות לתוצאות מרכזיות בתורת הבחירה החברתית, ביניהן משפט Arrow ומשפט Gibbard–Satterthwaite.

לנתן גם תרומות חשובות בקריפטואנליזה, והוא נחשב לאחד החוקרים המובילים בעולם בתחום זה. נתן ושותפיו פתחו טכניקות שבירה חדשניות של מגוון מערכות הצפנה סימטריות, אשר מעבר לעומקן המתמטי הינן בעלות חשיבות מעשית רבה. דוגמא מפורסמת לכך היא עבודתו של נתן עם אלעד ברקן ואלי ביהם, אשר חשפה חולשה משמעותית והביאה להחלפתו של מנגנון ההצפנה של הדור השני של תקשורת סלולרית.

נימוקי ועדת פרס Erdos להענקת הפרס לדורון פודר

דורון פודר הוא חוקר מעמיק החוקר בתפר שבין תורת ההסתברות, תורת החברות הגיאומטרית, ותורה ספקטרלית של גרפים ויריעות, ומטריצות מקריות. בעזרת שילוב יוצא דופן זה הצליח דורון להביא לפריצת דרך במספר תחומים.

אחת הבעיות שהניעו את מחקרו של דורון היא להבין כיצד נראה הספקטרום של גרף מקרי עם דרגה חסומה. הניסיון להבין סוגיה זו הובילה אותו לתוצאות מרהיבות שגולתן במאמר משותף עם פרזנצ'בסקי על ההתפלגות של תוצאת הצבה מקרית של פרמוטציות במילה בחבורה החופשית על k-יוצרים, ובפרט איפיון מדויק לאיזה מילים ההתפלגות המתקבל היא אחידה.

בעזרת תוצאות עמוקות אילו הצליח דורון לקבל תוצאות חזקות ואלגנטיות לגבי ספקטרום של גרפים מקריים בדרגה חסומה במספר מודלים.

כיוון מבטיח ומלהיב בעבודתו של דורון הוא השימוש בטכניקות של תורת החבורות הגיאומטריות להבנת התפלגות של הצבה מקרית של איברים בחבורות אוניטריות במימד גדול, ובכך קישר דורון באופן מרשים בין תורת החבורות הגיאומטריות לחקר מטריצות מקריות במימדים גבוהים.

בעבודותיו משלב דורון באופן עמוק ויצירתי מספר תחומים מתמטיים שונים, והישגיו לבדו ועם שותפים מצטרפים יחדיו למכלול מרשים.