“Petros Amca ve Goldbach Sanısı” ve Düşündürdükleri

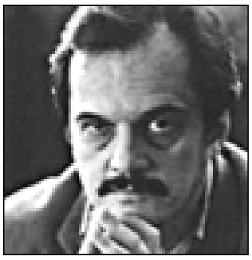
Cem Yalçın Yıldırım* / *yalciny@boun.edu.tr*

Apostolos Doxiadis’in **Petros Amca ve Goldbach Sanısı** adlı romanı[1] matematik etrafında dönüyor. Başlangıçta parlak bir matematikçi olan, anlatıcının amcası Petros Papahristou’nun Goldbach problemine musallat olmasının ve yaşamı boyunca bu problemi çözemeyip kendisiyle girdiği iddiayı kaybedişinin öyküsü.

Hardy, Littlewood, Ramanujan, Gödel, Turing, Carathéodory ve adı verilmeden Avusturyalı Rademacher gibi birçok tanınmış matematikçi karakter olarak serbestçe kullanılmış. Çoğu matematikçinin kafasında bu kişilere ilişkin imgeler zaten vardır, ama kitapta yüzeysel olarak serpiştirilen bu karakterler matematikçi olmayanlara ne ifade eder bilemiyorum.

Hemen her seferinde, haksızca, desteksizce, yüzeysel bir biçimde ve hatta arasıra galizce matematikçiler olumsuz karakterler olarak çiziliyor. Örneğin intihara eğilimli olmaları, bir probleme saplanıp kalmaları, “vasat matematikçi” olup “yürüyen trajedi” haline gelmeleri vb.

Kitaptaki karakterlerin ruhsal durumlarını matematiksel problemler derinden etkiler, ancak adlarının uyandırabileceği gizem dışında bu problemlerin en küçük bir açıklaması yok! Nitekim Petros Amca’nın tutkusu matematikten ziyade şan ve şöhrete yönelik: *Şu genç adama bir bak, hani **benim** – hâlâ bana ait diye düşünüyorum – doğal sayıların partisyonları teoremini benden önce yayımlayan Avusturyalı vardı ya, elde ettiği sonuçla acaba bir Hilbert’in, bir Poincaré’nin payesine yükseldi mi? Tabii ki hayır! Belki Matematik Sarayının arka odalarından birinde portresine bir yer edinebildi... Veyahut Hardy ve Littlewood’u düşün, ikisi de birinci sınıf matematikçiler. Herhalde Ünlüler Galerisine – çok geniş bir Ünlüler Galerisidir bu, dikkatini çekerim – çıkabildiler, ama heykellerini Sarayın ulu girişinde Evklides, Arkhimedes, Newton, Euler, Gauss’un heykellerinin yanına diktirmeyi başaramadılar. Benim tek emelim **buydu**, ve asal sayıların iyice derinlerdeki gizemlerini çözmek anlamına gelen Goldbach Kestirimi’nin ispatından daha azı bana bu yolu açamazdı*[2]... (s. 93)


Apostolos Doxiadis

Peki kim bu Doxiadis de böyle bir roman kaleme almış? Bilişim ağındaki sitesinde yazdığına göre 1953’te doğmuş. On beş yaşında New York’taki Columbia Üniversitesi’nin Matematik Bölümü’ne özgün bir makale sunarak girmiş, Paris’te lisansüstü düzeyde uygulamalı matematik çalışmış (tamamlayıp tamamlamadığı belli değil.) Sonradan kendini tiyatro, film ve edebiyata vermiş, uluslararası ödüller almış.

Burada saptamadan geçemeyeceğimiz bir olgu, hem Petros Amca’nın hem de Doxiadis’in dâhi çocuk olarak vasıflandırılıp umut vaadeden matematikçiler olarak yetiştirilmişken, ihtirastan dolayı Petros Amca’nın çözemeyeceği bir probleme saplanıp mesleki gelişimine ve gönül maceralarına sırtını dönüp içine kapanması, Doxiadis’in ise matematiği bırakmasıdır.

Doxiadis’in yansıtışından çıkarılabileceğinin aksine, matematikçilerin çoğu bunalım içinde değildir. En ünlülerden örnek vermek gerekirse, Pythagoras, Euler, Gauss, Hilbert, Hadamard ve daha birçok matematikçi uzun, verimli ve sağlıklı yaşamışlardır. Herhangi bir uğraşta ilerleme kaydetmek için tutkunun vazgeçilmez olduğu kesindir. Kitabın, matematik tutkusunun genellikle hastalıklı olduğu izlenimini vermeye yönelik olması herhalde yazarın travmalarından kaynaklanıyor.

Doxiadis’in yanlış fikirleri, üstelik birçok kişi-

* Virgül dergisinin Mart 2001 sayısında yayımlanan yazının aslına yakın bir uyarlamasıdır.

Boğaziçi Üniversitesi Matematik Bölümü öğretim üyesi.

1 Yunanca: “O Theios Petros kai i Eikasia tou Goldbach”, 1992, Kastioniotis. İngilizce: “Uncle Petros and Goldbach’s Conjecture”, Faber and Faber, 2000. Türkçe: Everest Yayınları, 2000, çeviren Devrim Denizci.

2 Bu ve aşağıdaki alıntılarda Türkçe çeviriden yararlandım. Bazı paragrafların İngilizcesi de elimdeydi, onların çevirisinde değişiklikler yapmayı uygun gördüm.

nin kolayca inanabileceği türden olanları bunlarla bitmiyor: *Bildiğiniz gibi, matematik bir genç oyunudur. Mükemmelliğe ulaşmak için genç olmayı şart koşan birkaç kişinin uğraşından biridir... (Bu açıdan spora çok benzer.) Matematik tarihinde otuz beş kırk yaşın üzerinde büyük buluşlara imza atanların sayısı çok azdır. Riemann otuz dokuz yaşında öldü, Niels Henrik yirmi yedisinde, Galois ise ne yazık ki yirmisinde; yine de isimleri matematik tarihinin sayfalarına altın harflerle yazıldı... Euler ve Gauss da teoremlerini ileri yaşlarda ortaya koymakla birlikte temel buluşlarını gençlik yıllarında yapmışlardı. Yirmi dört yaşındaki Petros, başka bir alanda çalışsaydı umut verici bir genç olabilirdi... Ama matematikte ancak yeni yeni gücünün doruklarındaydı... On yıl içinde başaramadığı takdirde gerçek bir Büyük Buluş için ihtiyaç duyulan icat yeteneğinin parlaklığı ve girişimci ruhun coşkusu, tamamen yok olmasa da, sönmeye başlayacaktı...* (s. 64-65; Niels Henrik'in soyadı unutulmuş, Abel olacak!)

Bu örnekler aslında öne sürülen savı baltalıyor! Galois yirmisinde düelloda öldüğüne göre ileri yaşlarda matematik yapamamaya örnek teşkil edemez. Euler ve Gauss'un ise ileri yaşlarda matematiksel sonuçlar çıkarmayı sürdürdükleri zaten belirtiliyor. Hem matematik artık o denli ilerlemiş ki, oluşmuş bilgi birikimini yirmi yaşına dek öğrenip üstüne yeni gelişmeler yaratmak mucize sayılmalı. Yüzelli yıl önce durum böyle değildi. Üstelik, matematiksel bilgi üretiminde olgunluğun getirileri öteden beri bilinir.

Konuda uzman olmayan okurları aldatabilecek bir nokta da şu: Petros, Riemann Hipotezi'ni küçümser (s. 66), onun için önemli olan Goldbach Kestirimi'dir. Hele hele Hardy ve Littlewood'un Riemann Hipotezi'ni varsayarak ispatladıkları teoremlere Petros'un itibar etmesi nasıl beklenebilir? (s. 71). İşin aslı şu: Riemann Hipotezi'ne dayanan ve matematiğin gelişiminde dönüm noktası olan teoremler vardır. Riemann Hipotezi, ortaya atıldığından beri geçen yüz kırk yıl boyunca birçok sonuçla desteklenmesine karşın ispatlanamamış merkezi konumda bir önermedir. İnsanların öngörülerini artırmak için ille de bu hipotezin ispatını beklemeleri mi gerekir? Üstelik bu hipotezi doğru varsayınca çıkan sonuçları irdelemek de pekâlâ saygın bir uğraştır. Asal sayılara ilişkin gizemler arasında Goldbach Kestirimi'nin Riemann Hipotezi'nden daha derinde olduğu matematikçiler arasında yaygın bir kanıdır. Riemann Hipotezi'nin asalların dağılımına ilişkin gerektirmelerini umursamadan Goldbach Kestirimi'ni ispatlamaya uğraşmak gerçekçi değildir. Yukarıdaki ilk alıntıda ima edilenin tersine Riemann Hipotezini ispatlayabilenin heykeli Sarayın ulu girişinde yer alacaktır.

Birkaç ufak hataya da (bazıları çeviri esnasında ortaya çıkmış olabilir) çabucak değineyim. Hilbert'in en önemli diye ilan ettiği problemlerin sayısı otuz üç değil yirmi üçtür (s. 130); Pythagoras teoremindeki eşitlik $x^2 + y^2 = z^2$ biçimindedir (s. 161); Gauss'un ve ondan sonra gelenlerin asal sayı teoremine varmak yolunda doğru bir adım atamadıkları (s. 69) ve herhangi bir zaman diliminde dünyanın tek sayı kuramcısı olarak Hadamard'ın kabul edildiği (s. 72) düpedüz yanlıştır. Şaka yollu sözü geçen (s. 35) Nobel matematik ödülü diye birşey yoktur. Bir de eklemeliyim ki Dört Renk Teoremi ve Fermat'nın Son Teoremi kitabın dediğinin (s. 130) aksine ispata kavuşmuş durumdadırlar. Kitapta Fermat'nın Son Teoremi'nin 1993'te ispatlandığı her nedense ancak 161. sayfada yazarın dipnotunda verilmiş. Dört Renk Teoremi (bir haritada ülkeler – şekilleri nasıl olursa olsun – komşu ülkeler farklı renkler olması koşuluyla dört renge boyanabilir önermesi; komşudan kastedilen bir eğri boyunca komşuluktur, bir veya birkaç noktada birbirine değen ülkeler komşu sayılmıyorlar) 1976'da Appel ve Haken tarafından bilgisayar marifetiyle ispatlanmıştır. Bilgisayar kullanılmasının nedeni ikibin kadar hali hızlıca denetleyebilmek içindir. Bu halleri tespit edenler ve gerekli bilgisayar programını yazanlar matematikçilerdir, yani bir yapay zekâ uygulaması söz konusu değildir.

Matematikçilere ilişkin edindirdiği yanıltıcı, eksik, genelleyici izlenimler ve uzmanların hemen tepki göstereceği yanlış lafların dışında, diyebileceğim, Doxiadis zekice ve sürükleyici bir kurgu kurduğu. Ayrıca matematikçi ruhunu doğru verdiği bölümler de yok değil. Örneğin Petros Amca matematikçi olmayı düşünen yeğenine yaz tatili ödevi olarak Goldbach problemini verir (sorunun adını ve ününü belirtmeyerek), çocuk çok uğraştıktan sonra yenilgiyi kabullenir. Yıllar sonra, Petros Amca bu ödevi vermekteki amacının çocuğun problemi çözüp çözemeyeceğini sınamak değil, gerekli tutkuyu taşıyıp taşımadığını açığa çıkarmak olduğunu söyler: *Üstün başarı için gerekli – ama seni temin ede-*

rim, yeterli olmayan – ilk önkoşul kararlılıkla kendini adamaktır. Eğer sahip olmayı arzuladığın yetenek gerçekten içinde olsaydı, sevgili evlat, gelip benden inayet istemezdin, kendi başına gidip yapardın. Bu, durumunu ilk ele veren alametti!.. Uzak bir ihtimalle senin hakkında yanılmış olsaydım, ve sen gerçekten yüce olmak için seçilmiş olsaydın, bu deneyim seni ezmezdi. Aslında senin tabirinle "dehşetengiz" değil, bilakis heyecan, ilham ve yaşamgücü verici olabilirdi... Ama sen... Sen çözümü soracak merakı bile göstermedin! (s. 127-128).

Kitap matematik dergilerinde ve baktığım bazı bilişim ağı sayfalarında genellikle olumlu karşılanmış. Herhalde bunun esas nedeni başkişileri matematikçi olan romanların azlığı dolayısıyla bu kitabın "medyatik"likten çok uzak olan matematiğin gündeme gelmesine olan katkısı. Kitabın İngilizce yayıncısı Faber & Faber, 1742'den beri çözülemeyen Goldbach problemini 15 Mart 2002'ye dek çözene bir milyon dolar ödül verecekti.

Velhasılkelam Petros Amca Goldbach problemine belasını satmış diyorum. Yazarın matematiğe karşı hıncı olduğuna inanıyorum. Ortaya koymuş olduğum üzere, kitabın yanlışlarla dolu olması da cabası. Okurlara Hardy'nin **Bir Matematikçinin Savunması**, J.P. King'in **Matematik Sanatı**, Sinan Sertöz'ün **Matematiğin Aydınlık Dünyası** ve Cemal Yıldırım'ın **Matematiksel Düşünme** adlı kitaplarını öneririm.

Gelelim çeviriye. Yığınla dizgi hatasını ve basit yanlışı belirterek burada vakit tüketmek yerine, daha hassas bir konunun, matematik terimlerinin Türkçeye çevirisi üzerinde duralım. Bence İngilizce "conjecture" sözcüğüne karşılık olarak "sanı" yerine "kestirim" daha uygun. "Sanı" daha çok duygularda ve kişisel anlamlar dünyasında gibi, öte yandan "kestirim" düşünceye ve çözümlemeye dayalı tahmin anlamını veriyor. Çevirmen dilimizde yerleşmiş birçok terimi bilmiyor. Örneğin "sayı kuramı", "paralelogram", "çelişkisizlik ispatı", "basit analiz", "grup tasviri", "doğal sayıların parçalanması" diyor ki, bunların doğruları sırasıyla şöyle: "sayılar kuramı", "paralelkenar", "tutarlılık ispatı", "analize giriş", "grup temsilleri", "doğal sayıların partisyonu". *Reductio ad absurdum*'un Türkçesi var, "olmayana ergi". Hele "e. prof"taki e.'nin "eski"nin kısaltması olarak belirtilmesine ne demeli; "e. prof", "professor emeritus"un kısaltmasıdır, "memuriyet unvanını sürdüren emekli profesör" anlamına gelir. En vahimi "karmaşık sayılar"a (complex numbers) ilişkin hatalar: İlk olarak 70. sayfanın dipnotunda "karmaşık sayılar" yazar tarafından doğru tarif ediliyorsa da, "gerçel sayı" ve "sanal" olması gereken sözcükler yerine çevirmen "gerçek sayı" ve "düşsel" kullanmış; sonra 102. sayfada "karmaşık sayılar" terimi "asal olmayan sayılar"a (composite numbers) karşılık geliveriyor! 106. sayfanın dipnotunda çevirmen çok basamaklı sayıları yazarken nokta ve virgüllerin kullanılışını bilmediğini gösteriyor. Ayrıca 70. sayfanın ilk paragrafında "sonsuz bir hesaplama yöntemi" ve "karmaşık sayılar düzlemine uygulanan son derece küçük hesaplar" gibi hiçbir anlam ifade etmeyen ifadelerle karşılaştım. Son olarak bir de şu komiklikten sözedeyim: 59. sayfada "ihtiyar Ramanujan" deniyor, ama Ramanujan 32 yaşında öldü (s. 72); İngilizce'de "old" bazan "dostumuz" ya da "emektar" anlamında kullanılır.

* * *

Tarihte asal sayı kavramına ilk Eski Yunan'da rastlıyoruz. Eski Yunan uygarlığı, Thales ve Pythagoras'ın öncülüğünde (M.Ö. 6. yüzyıl) matematiği Mısır ve Babil'den öğrendi. Çok geçmeden matematik Yunan filozoflarınca tartışılır oldu. Buldukları sonuçların yanısıra, süreklilik, hareket, sonsuzluk, herhangi bir uzunluğun seçilmiş bir birim cinsinden ölçülebilmesi gibi, matematiksel kavramların içerdiği zorlukların farkına varmaya başladılar. Böylelikle matematiksel ispat ve aksiyomatik yapı anlayışları doğdu. Bilindiği kadarıyla ispatın ilk örneklerini geometride Thales verdi. Sonra Pythagoras (ya da onun kurduğu okul) diküçgenler için Pythagoras Teoremi'ni ve bu teoremden yola çıkarak dikkenarları birim olan diküçgenin hipotenüsünün uzunluğu olan $\sqrt{2}$'nin irrasyonelliğini (yani iki tamsayının oranı olarak ifade edilemediğini) gösterdi.

O zamandan beri matematiksel ispat denince bir önermenin, doğruluğu aşikâr olan (ya da varsayılan) daha basit önermelerden uygun mantık zincirinin kurulması sonucu gösterilmesini anlıyoruz. İspatın en önemli özelliklerinden birisi kalıcılığıdır: Matematikte doğru bilinenler değişmezler (bilimlerin tersine), zamanla bunların üzerine yeni bilgiler eklenir. Matematikte doğru bilinenlerin değişmezliği matematikçileri uğraşlarının evrenselliğine inandırır. Bu noktada şu soru hemen akla gelebilir:

Bir ispatın doğru olduğuna nasıl emin olabiliriz? İspatlandığı iddia edilen çıkarım birçok kişi tarafından incelenir, hiç yanlış bulunmazsa (ya da bulunan yanlışlar düzeltilebilirse) matematikçiler zamanla ispatın geçerliliği yönünde hemfikir olurlar ve o çıkarıma ispat denmeye başlanır.

Zaten $\sqrt{2}$ ya da $(1+\sqrt{5})/2$ (altın oran) gibi irrasyonel sayılarla geometrik problemler yüzünden tanışan Eski Yunanlılar, belki de irrasyonel sayı kavramının getirdiği zorluklardan ötürü, matematiğin temel ögeleri olarak sayıların yerine geometrik kavramları (nokta ve doğru) görmeyi seçtiler. Sözü geçen zorluklarla başa çıkmak için Evdoksos geometrik süreklilik (continuum) kuramını ortaya attı. Şimdi bize apaçıkmış gibi gelen bir doğrunun deliksiz olarak noktalardan oluştuğunu söyleyen bu kuramın getirdiği gelişim düzeyi ancak 19. yüzyılda kurulabilen irrasyonel sayılar kuramıyla aşılabildi. Eski Yunanlılar matematikte bildiklerini, varsayımlardan başlayıp sonuçlara varan dizgesel bir yapıya kavuşturmaya çalıştılar. Bu çalışmalar Evklides'in (M.Ö. 4. yüzyıl) kitaplarıyla doruğa ulaştı. Matematik artık yalnızca uygulama amaçlı bilgiler yığını olmanın ötesine geçmiş, salt kendisi için de yapılmaya başlanmıştı. Eski Yunanlıların geometrik yaklaşımları, sonradan temel konumu ele geçiren sayı ve cebirsel işlem kavramlarını büyük ölçüde ıskalayarak matematiğin ve bilimlerin gelişmesine ket vurdu. Yine de asal sayılar hakkındaki en temel teoremler Evklides'in kitaplarında ortaya çıkmıştı. Evklides yazmamasına karşın herhalde her tamsayının bir ve yalnız bir şekilde asal çarpanlara ayrılabildiğini (*aritmetiğin temel teoremi*) biliyordu. Üstelik Evlikdes asal sayılar dizisinin sonsuzluğunu ispatladı. Eski Yunan'da sayılar kuramının son sesi Diofantus'tan (M.S. 3. yüzyıl) geldi. Sonra sayılar kuramı karanlık çağlara girdi, ta ki Diofantus'un İskenderiye yangınından beri kayıp kitaplarının bazıları bulunana ve Bachet tarafından 1621'de Latinceye çevrilene dek (Diofantus'un on üç kitabından altısı 1464'de Almanya'da bir kütüphanede ortaya çıktı ve astronom Regiomantus'un eline geçti. Son yıllarda Diofantus'un dört kitabı daha ortaya çıkmıştır.) Kısa süre içinde bu kitapları okuyup etkilenen Mersenne ve Fermat'dan başlayarak asal sayılar ve sayılar kuramının diğer konuları günümüze dek uzanan hızlı gelişme dönemine girdi.

1742'de, matematikte adı başka hiçbir yerde geçmeyen Goldbach, meşhur Euler'e yazdığı bir mektupta, 2'den büyük her çift sayının iki asalın toplamı olarak ifade edilebileceğinin ispatını, ya da bu önermenin yanlışlığının ispat veya örnek yoluyla gösterilmesini istedi. Goldbach denediği bütün örneklerde önermenin tuttuğunu görmüştü ($4 = 2 + 2$, $16 = 5 + 11$, $114 = 7 + 107$ gibi.) Aradan geçen çeyrek binyılda kimse *Goldbach Kestirimi* denilen bu önermeyi veya aksini ispatlayamadı. Buna çok yakın olan ikiz asallar dizisinin sonsuzluğu önermesi de ispatlanamadı (ikiz asallar, aralarındaki fark sabit olan asal sayı çiftleridir; 5 ve 7, 17 ve 19, 101 ve 103 gibi.) Dile getirilişi çok kolay olan bu tür önermelerin tüm insanlık için en zor problemler kümesinde yer aldığı anlaşıldı. Zorluğun temel nedeni yalınlıkla şöyle belirtilebilir: Asal olmak, tanımı gereği, çarpımsal bir özellik iken, Goldbach veya ikiz asal problemlerinde toplama işlemi işin içindedir.

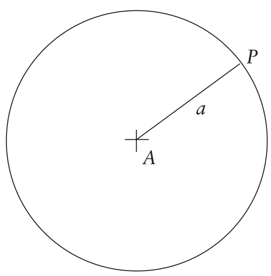
Euler, Goldbach Kestirimini ispatlayamadıysa da, asal sayılar dizisi ve tüm doğal sayıların dizisi arasında ilişkiler veren analitik ifadeler buldu. Sonradan Riemann'ın (1859) çığır açıcı fikirleri bunlardan kaynaklandı. Arada geçen sürede en önemlileri Gauss, Legendre, Dirichlet, Çebiçev ve Mertens tarafından olmak üzere *asal sayı teoremi* hakkında çalışmalar yoğunluk kazandı. İlk Gauss'un tahmin ettiği bu teorem (1792), genel olarak, x çok büyük bir sayıysa, 1'le x arasında *yaklaşık* $x/\ln(x)$ tane asal sayı olduğunu söyler. Asal sayı teoreminin ispatı, ancak Riemann'ın tanımladığı ve bazı özelliklerini gösterdiği *zeta fonksiyonu*'nun iyice incelenmesiyle, 1896'da Hadamard ve de la Vallée Poussin tarafından ayrı ayrı verildi. Riemann, zeta fonksiyonuna ilişkin bazı önermeleri ispatsız yazmıştı. Bunlardan biri dışında hepsi zamanla ispata kavuştu: Karmaşık sayılar düzleminde tanımlanmış zeta fonksiyonunun sağ yarı-düzlemde sıfır değerini aldığı noktaların tümünün bir doğru üzerinde (gerçel kısmı 1/2 olan noktaların doğrusu) bulunduğu önermesi ise ispatsız kaldı, ve *Riemann Hipotezi* adıyla anılır oldu. Riemann'ın açtığı yol 20. yüzyılda kâh zeta fonksiyonunun yeni özelliklerinin keşfine, kâh asal sayı teoremindeki hata payının ayrıntılı olarak incelenmesine ve yeni kestirimlerin ortaya çıkmasına olanak sağladı. Riemann zeta fonksiyonu, birçok özelliğinin asal sayıların dağılımıyla karşılıklı ilişkiler içinde olmasının (hatta belki de asal sayılara ilişkin herşeyi kodlamasının) dışında, genellemeleriyle birlikte matematiğin başka dallarında ve kuantum mekaniğinde de rol sahibi oldu. Vinogradov (1937) *yeterince büyük* (ama buna belli bir değer vermeksizin) her tamsayının en çok dört asalın toplamı olarak yazılabileceğini gösterdi. Schnirelmann ise 1931'de 2'den büyük *her* tamsayının en çok üç yüz bin asalın toplamı olarak yazılabileceğini ispatlamıştı (üçyüzbin şimdi yediye indirilmiş durumda.) Goldbach problemine en yakın sonuçlardan biri de 1973'te Chen'in yeterince büyük her çift sayının bir asal ve bir de en çok iki asal çarpanı olan bir sayının toplamı olarak ifade edilebileceğini ispatı oldu. Ama hâlâ Goldbach Kestirimi'nin yakın gelecekte çözümü için pek umut yok.

1931'de Gödel, matematiği ve felsefeyi sarsan iki "eksiklik teoremi" ispatladı: 1) Doğal sayılarda doğru olan ama ispatlanamaz (toplama ve çarpmayla ilgili) önermeler vardır ve 2) Aritmetiğin tutarlılığı aritmetiğin kendi içinde ispatlanamaz. Eksiklik teoremlerinin etkisiyle Goldbach Kestirimi ve Riemann Hipotezi'nin üzerinde karara varılamayacak olasılığı olsa da, bu görüşün sayılar kuramcıları arasında çok taraftarı yoktur (ama ünlü matematikçi Knuth, Goldbach Kestirimi'nin Gödel'in varlığını gösterdiği ispatlanamayacak teoremlerden biri olduğuna inanmaktadır.) Goldbach Kestirimi'yle matematiğin temelleri arasında bazı ilişkileri irdeleyen Pogorzelski'nin çalışmalarının sayılar kuramını etkileyecek bir duruma geldiğini sanmıyoruz.

Matematiğin birçok dalında büyük gelişmelere yol açmış olan Gauss, matematiğin bilimlerin kraliçesi, sayılar kuramının da matematiğin kraliçesi olduğunu söylemişti. Kronecker de "Tanrı doğal sayıları yarattı, diğer herşey insan ürünüdür" demişti. İmdi asal sayılar hakkında bilinenlerin uygulamaları var mı diye merak edenler olabilir. Sayılar kuramcılarının çoğu bir problemle uğraşırken uygulamalara ilişkin kaygı taşımazlar. Matematiğin matematik için yapılmasına en çok değer verip, uygulamalara omuz silkenlerin başında Hardy gelir. Ne var ki, Hardy'nin çok sevdiği asal sayılar artık şifrelemede, bilişim ağındaki güvenliği sağlamakta kullanılmaktadır. Bunun neye dayandığı kolaylıkla açıklanabilir. Size iki asal sayı verilse (diyelim 97 ve 89) bunların çarpımını ($97 \times 89 = 8633$) hemen bulabilirsiniz. Ama size 8633 sayısı verilip bunun asal çarpanları sorulsa 97 ve 89'u bulmanız daha zor olur. Sayılar büyüdükçe bu iş iyice zorlaşır, öyle ki bilinen en büyük asallar (bugün, $2^{13466917} - 1$ bilinen en büyük asal olma rekorunu elinde tutuyor) kullanıldığında aynı soruyu yanıtlamak bilgisayarların bile binlerce yılını alacaktır. Böylelikle iki büyük asal alıp, bunları çarpınca çıkan sayıyı tüm dünyaya ilan edersiniz, ama kimse çarpanlarını bulamaz. Sayılar kuramının en kolay bazı teoremlerinin yardımıyla, bu olgu yalnızca istediğiniz kişilerin kırabileceği bir şifreye sahip olmanızı sağlar. Bu konuda geçen yıl önemli bir gelişme oldu. Üç Hintli matematikçi (Agrawal, Kayal ve Saxena) verilen bir tamsayının asal olup olmadığına nispeten kısa zamanda (polinom-zamanlı) koşulsuzca karar veren bir algoritma buldular (daha önce Riemann Hipotezi'nin doğruluğu koşulu varsayılarak bu yapılabiliyordu.)

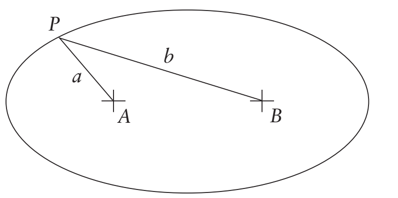
Ad astra per aspera! ♥

Çember



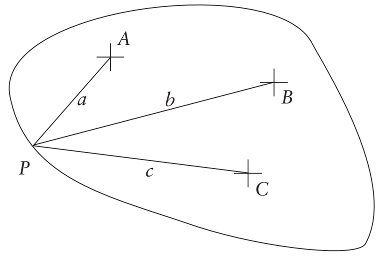
Verilen bir A noktasına uzaklığının karesi sabit (a^2) olan noktalar (P) kümesi bir **çember**dir.

Elips



Verilen A ve B noktalarına uzaklıklarının karelerinin (a^2 ve b^2) toplamı sabit (r^2) olan noktalar (P) kümesi bir **elips**tir.

???



Verilen A, B ve C noktalarına uzaklıklarının karelerinin (a^2, b^2 ve c^2) toplamı sabit (r^2) olan noktalar (P) kümesi nedir?