Kapakta: Asal Portreler

Olcay Coşkun / olcaycoskun@gmail.com

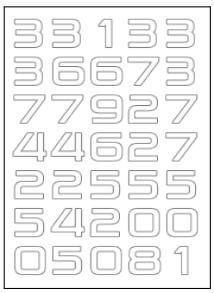
"Sayılarla boyama" bulmacalarını özellikle küçük yaştaki çocuklar çok severler. Bu tür bir bulmaca hazırlamanın algoritması basittir: Önce bir resim seçilir; bu resim yap-boz parçaları gibi, ama resim tanınacak biçimde parçalanır; aynı renge boyanması gereken parçalar aynı sayıyla numaralandırılır; renk kodları verilir ve bulmaca hazır!

Bu basit bulmacaların yanı sıra özellikle son yıllarda yaygınlaşan ve uzakdoğu kültürünün önemli bir parçası olan mandalalardan da söz edebiliriz. Britannica'ya göre mandala, Sanskritçede çember demektir ve Hindu ve Budist Tantrizm'inde kutsal ayinlerde ya da meditasyonlarda kullanılan bir araçtır. Evrenin bir temsilidir [2].

Modern çağın renkli kalem üreticileri, bu derin anlamdan ari, yazılımların ürettiği binlerce mandalayı bizlere sunmaktadır. Bu düzeydeki mantık çocuk bulmacalarıyla aynıdır. Geometrik şekiller bir araya getirilerek simetrik bir resim oluşturulur ve renklendirme tamamen okuyucuya/boyacıya bırakılır.

Abel'in Asal Portreleri

MIT'den Zachary Abel asal sayıları renk seçim aracı olarak kullanan asal portreleri keşfetti [1]. Abel'in yöntemi çok basamaklı asal sayı $r_1 r_2 \dots r_{n\times m}$'yi birim karelere ayrılmış $n \times m$ boyutundaki dikdörtgene, soldan sağa ve yukarıdan aşağıya yazarak başlıyor. Her rakama bir renk atayıp oluşan dikdörtgeni boyamayla sonlanıyor. Aşağıda 35 basamaklı bir asal sayının 7×5 boyutundaki bir dikdörtgene yerleşimi görülmektedir.

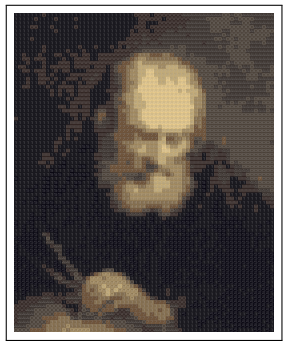


Her bir birim kareyi bir piksel gibi düşünürsek elde ettiğimiz sonuç çok düşük çözünürlükte bir resim olabilir. Yukarıdaki dizilimi değişik renk seçimleriyle renklendirerek desenler oluşturmayı deneyebilirsiniz!

Daha iyi çözünürlük elde etmek için en azından birkaç bin basamaklı asallar kullanmamız gerekir. Tabii ki bu kolay uygulanabilir bir yöntem değildir.

Meertens'in Algoritması

Arayışımıza bir asal sayı yerine bir resimle başlamak daha kolay sonuç almamızı sağlayabilir. Roland Meertens, Abel'in yöntemini Python koduna çevirmek için bu yaklaşımı benimsemiş [3]. Asal portresini bulmak istediğimiz fotoğrafı ve çözünürlük katsayısını Meertens'in programına veri olarak giriyoruz. Program fotoğrafı öncelikle, belirttiğimiz katsayıya bağlı olarak karelere ayırıyor. Her rakama bir renk atayacağımız için, program elde ettiğimiz karelenmiş fotoğrafın en çok 10 renk içeren yaklaşık versiyonlarını oluşturuyor. Bu esnada, doğal olarak, görsel bir miktar deforme oluyor. Asal sayı bulmayı kolaylaştırmak için deforme etme aşamasındaki renk seçimleriyle oynayarak, aynı fotoğrafın yüzbinlerce yaklaşık versiyonu elde ediliyor.



Fotoğraf 1: Arşimet.

Fotoğrafın bu şekilde numaralandırılmasıyla ortaya çıkan sayı asal sayıysa program başarılı bir asal portre elde etmiş oluyor. Sayı asal değilse, sıradaki yaklaşık versiyonla devam ediliyor.

Her ne kadar program kodunun önemli bir bölümü fotoğrafla ilgili olsa da aslında programın en önemli adımı, belirtilen çözünürlüğe göre ortaya çıkan ve binlerce basamaktan oluşan sayıların, asal olup olmadıklarının kontrol edildiği adımdır. Meertens'in algoritması bunun için Miller-Rabin

asallık testini kullanıyor [6]. (Aşağıda bu olasılıksal testi kısaca açıklayacağız.) Algoritma, testi her sayı için defalarca uygulayarak sayının asal olduğuna neredeyse emin oluyor.

Sonuçlarsa çok etkileyici. Dergimizin kapağındaki Gauss portresinin arkasında tam 10.729 basamaklı bir asal sayı var. (Kendi Gauss portrenizi yaratabilmeniz için bu portrenin boyanmamış bir versiyonunu da sizlere hediye ediyoruz.) Ayrıca bu yazıda gördüğünüz diğer bütün portreler de aynı program kullanılarak üretildi. Bu portrelerin yüksek çözünürlüklü sunumlarına web sayfamızdan erişebilirsiniz. Siz de Meertens'in web sayfasından program kodunu indirip kendi portrenizi üretebilirsiniz!

Programın çalışması üzerine son bir not. Kapaktaki portreyi bulabilmek için bilgisayarın üç gün çalışması gerekti. Yazıdaki diğer portrelerin çözünürlüğü düşük olduğundan onları daha kolay (birkaç saat içinde) bulduk.

Fotoğraf 2: Sofia Kovalevskaya.

Miller-Rabin Asallık Testi

Bu test kendi başına da ilginç olup, birçok uygulamaya sahiptir. Test, bir sayının bileşik olduğu sonucuna ulaşabilmesine karşın, asal sayı olmayı sadece (yüksek bir) olasılık olarak verir. Yani aslında bir bileşiklik testidir.

Miller-Rabin testinin temelinde Fermat'nın Teoremi bulunmaktadır.

Fermat'nın Teoremi: *N bir asal sayıysa*

$$a^N \equiv a \ (mod\ N)$$

denkliği her $0 \le a \le N-1$ için doğrudur.

Bu teoremi kullanarak, denkliği sağlamayan bir a sayısı bulup, N'nin asal olmadığını gösterebiliriz. Ancak asal olmamasına karşın teoremin sonucunu sağlayan sayılar da bulunur. Bu sayılara *Carmichael sayıları* denir ve en küçüğü 561'dir.

Buradaki açığı kapatmanın yolunu Miller-Rabin testi vermektedir [4, 5]. Testin temelini oluşturan gözlemi kısaca verelim.

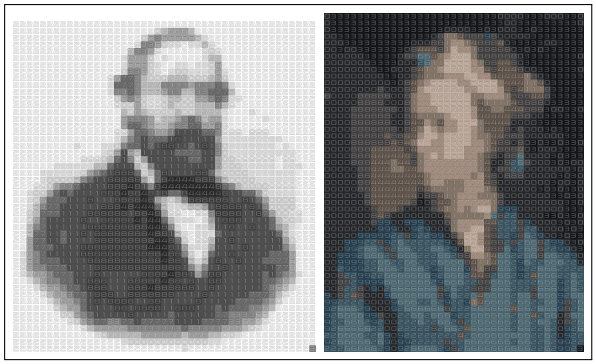
$p = 2^k s + 1$ asal, s tek ve $a \not\equiv 0 \pmod p$ ise, aşağıdakilerden biri mutlaka doğrudur:

1. $a^s \equiv 1 \pmod p$.
2. $a^{2^i s} \equiv -1 \pmod p$ denkliğini sağlayan bir $i \in \{0, 1, \ldots, k-1\}$ vardır.

Dolayısıyla verilen bir $N = 2^k s + 1$ sayısı için,

1. $a^s \not\equiv 1 \pmod N$ ve
2. her $0 \le i \le k-1$ için $a^{2^i s} \not\equiv -1 \pmod N$

koşullarını sağlayan bir $a \not\equiv 0 \pmod N$ tamsayısı (*şahit*) bulabilirsek N'nin bileşik olduğu sonucuna varırız.



Fotoğraf 3: Bernhard Riemann (solda), Leonard Euler.

Testin etkinliğini şahitlerin sıklığı belirler. Rabin'in bir sonucuna göre bileşik tek sayı N için 0 ile $N-1$ arasındaki sayıların en az yüzde 75'i şahittir [5]. Oysa N asal sayıysa hiçbir şahit bulunamaz.

Dolayısıyla testi yeterince çok sayıda a için denersek N sayısının çok büyük olasılıkla asal olduğu sonucuna varırız. Örneğin, bileşik sayı N için iki farklı a değeri ile testi uyguladıktan sonra testin hatalı sonuç verme (yani N'nin asal olduğunu verme) olasılığı $(\frac{1}{4})^2$ olur.

Bir Örnek

Yazımızı Miller-Rabin testini bir örnek üzerinde göstererek bitirelim. İşlemler çok uzun olmasın diye $N = 1057$ alalım ve

$$N = 2^5 \cdot 33 + 1$$

olarak yazalım. Hatırlarsanız şahitlerin N ile aralarında asal olması gerekiyor. Seçebileceğimiz en küçük şahit adayı olan $a = 2$ seçimini yapalım. Bu durumda $2^{33} \pmod{1057}$ kalan sınıfını hesaplamalıyız.

Modüler aritmetikten iyi bilinen bir sonuç

$$a \equiv b \pmod n \text{ ve } c \equiv d \pmod n$$

denklikleri sağlandığında $ac \equiv bd \pmod{n}$ denkliğinin de sağlandığını verir. Dolayısıyla yukarıdaki kalan sınıfını hesaplamadan önce parçalayabiliriz.

Basit çarpma işlemiyle $2^{10} = 1024 \equiv -33 \pmod{1057}$ buluruz. Dolayısıyla

$$2^{20} = (2^{10})^2 \equiv (-33)^2 \equiv 32 \pmod{1057}$$

ve

$$2^{30} \equiv (-33) \cdot 32 \equiv 1 \pmod{1057}$$

elde ederiz. Son olarak $2^{33} \equiv 8 \pmod{1057}$ bulunur. Bu sonuç $a = 2$'nin ilk koşulumuzu sağladığını gösteriyor.

Fotoğraf 4: Emmy Noether.

İkinci koşul için $i = 0, 1, 2, 3, 4$ sayıları için

$$2^{2^i \cdot 33} \not\equiv -1 \pmod{1057}$$

olduğunu görmeliyiz.

$\underline{i = 0}$ $2^{33} \equiv 8 \not\equiv -1 \pmod{1057}$.

$\underline{i = 1}$ $(2^{33})^2 \equiv 8^2 \equiv 64 \not\equiv -1 \pmod{1057}$.

$\underline{i = 2}$ $(2^{33})^4 \equiv (2^6)^2 \equiv 925 \not\equiv -1 \pmod{1057}$.

$\underline{i = 3}$ $(2^{33})^8 \equiv (2^6)^4 \equiv 32 \cdot 16 \not\equiv -1 \pmod{1057}$.

$\underline{i = 4}$ $(2^{33})^{16} \equiv 2^{18} \equiv 8 \not\equiv -1 \pmod{1057}$.

Böylelikle ilk denememizde bir şahit bulduk ve $N = 1057$'nin bileşik sayı olduğu sonucuna ulaştık.

Yazıda kullanılan üretilmiş portrelerin asılları Britannica web sayfasından alınmıştır. Asal portreler kodunu kullanmamıza izin verdiği için Roland Meertens'e teşekkür ederiz.

Kaynaklar

[1] Abel, Z., "Prime portraits", Proceedings of the 19th Annual Bridges Conference, Jyväskylä, Finland, 359–362 (2016).

[2] Britannica, https://www.britannica.com/topic/mandala-diagram (3 Eylül 2021 tarihinde erişildi.)

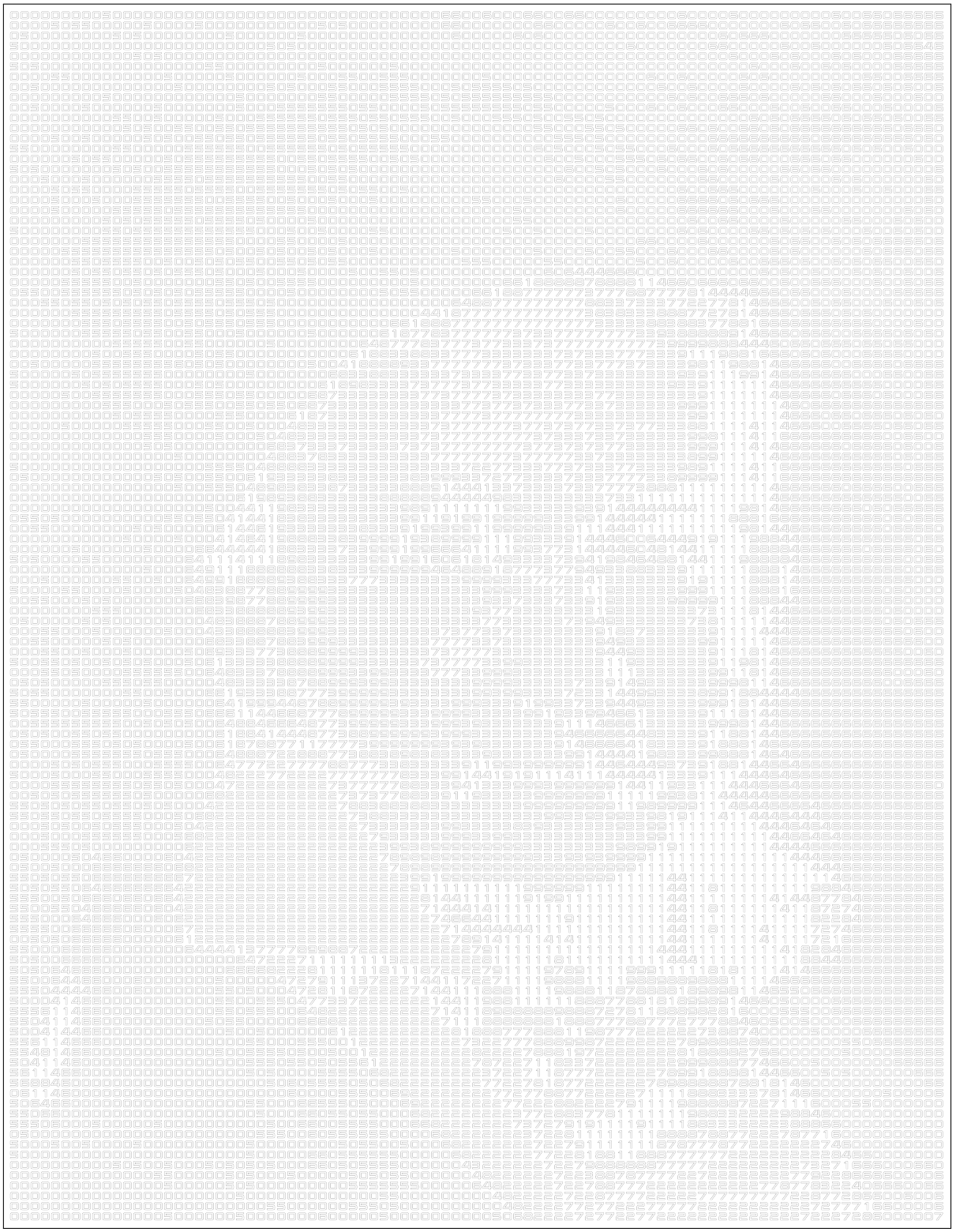
[3] Meertens, R., Painting by Prime Number, http://www.pinchofintelligence.com/painting-by-prime-number/

[4] Miller, G. L., "Riemann's Hypothesis and Tests for Primality", Journal of Computer and System Sciences, 13 (3) 300-317 (1976).

[5] Rabin, M. O., "Probabilistic algorithm for testing primality", Journal of Number Theory, 12 (1) 128-138 (1980).

[6] van Tilborg, H. C. A., 'Encyclopedia of Cryptography and Security", Springer, 2005.

Fotoğraf 5: Cem Yalçın Yıldırım.



Fotoğraf 6: Carl Friedrich Gauss.