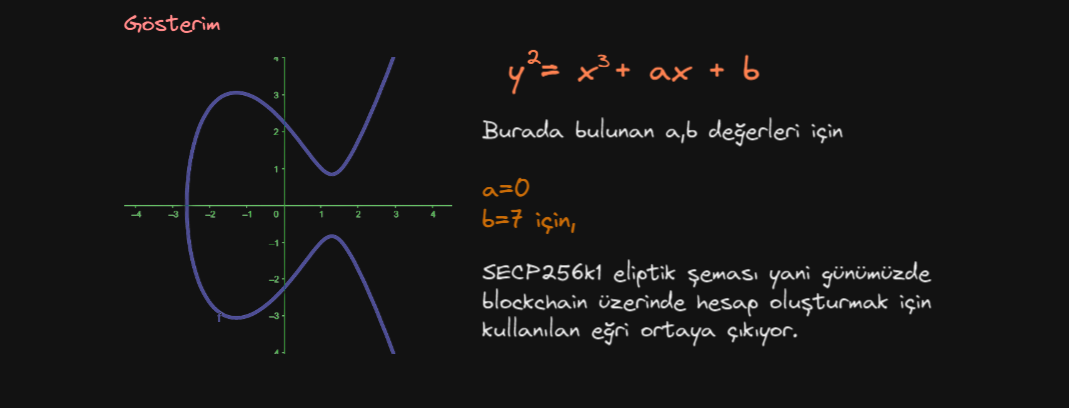


Kriptoloji

Eliptik eğri kriptografisi (ECC), şifreleme anahtarının herkese açık, şifre çözme anahtarının ise gizli tutulduğu modern bir açık anahtarlı kriptografi türüdür. Bu özel strateji, her türlü şifrelenmiş ürün için güvenlik sağlamak üzere eliptik eğrilerin doğasını kullanır. ++

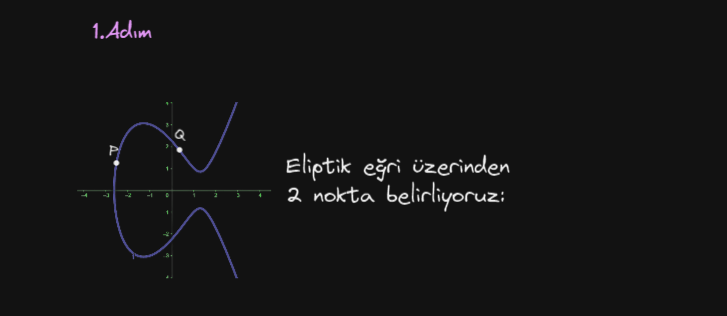
Eliptik eğrilerin genel formülünde belirli katsayıları kullanarak oluşturduğumuz ve hala günümüzde kullanılan SECP256k1 eliptik eğri şeması, Bitcoin hesapları oluşturulurken de kullanılmaktadır. +++

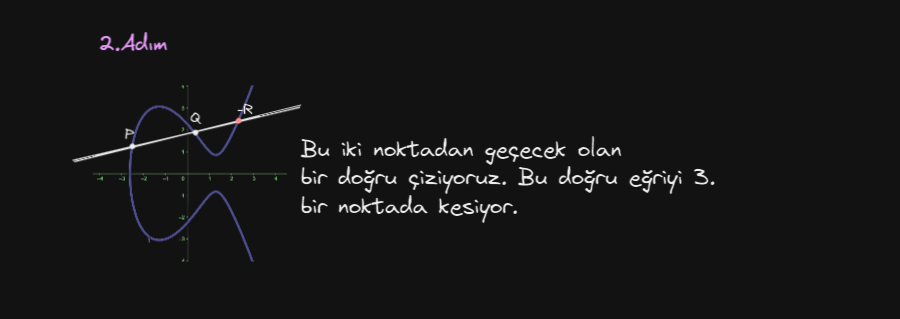


Eliptik Eğrilerde kriptoloji konuşmadan önce ufak bir matematiksel modelleme oluşturalım. Herhangi iki noktayı eliptik eğriler üzerinde nasıl toplarız? ++

Eliptik eğri, üssel ifadesinden kaynaklı olarak sağladığı kolay girdi çıktı dengesi sayesinde

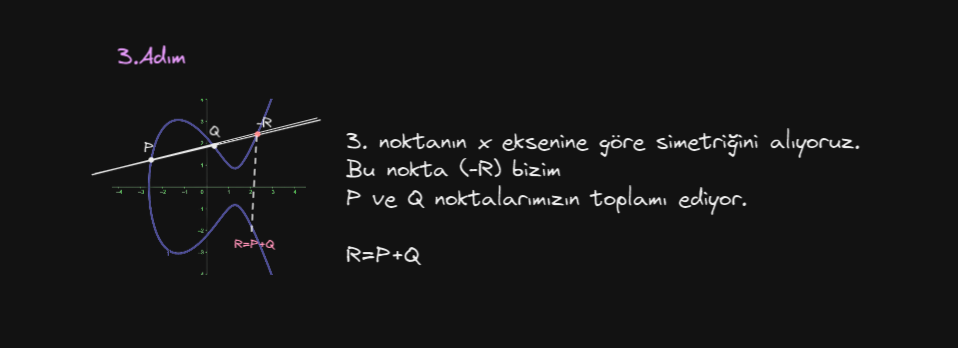
popüler olarak sistemlerde kullanılmaktadır.+++

İlk adım olarak eliptik eğri üzerinde birbirinden farklı konumda iki nokta seçiyoruz.+++

İkinci adım olarak bu iki noktadan geçen bir doğru çiziyoruz. Bu doğru eliptik eğrilerin doğası gereği, eğriyi 3. Bir noktada kesiyor.+++ 

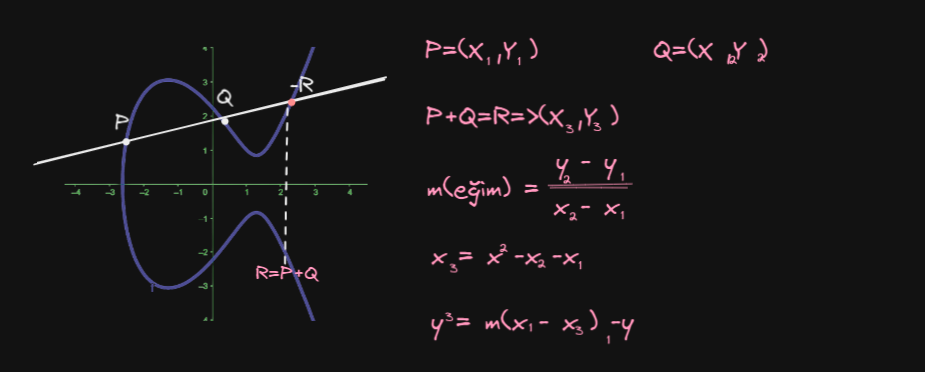
Üçüncü adım olarak -R olarak bulduğumuz 3. Noktanın x eksenine göre yansımasını alarak yeni bir nokta elde ediyoruz. Bu noktayı R olarak adlandırıyoruz.

R=P+Q şeklinde sonuca ulaşıyoruz.+++



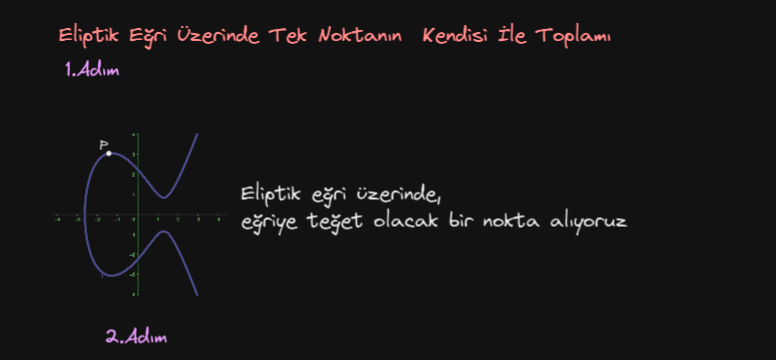
Meraklısına:

“Ateş, bunun arkasında yatan matematik ne?” Diyorsanız buyrun:+++

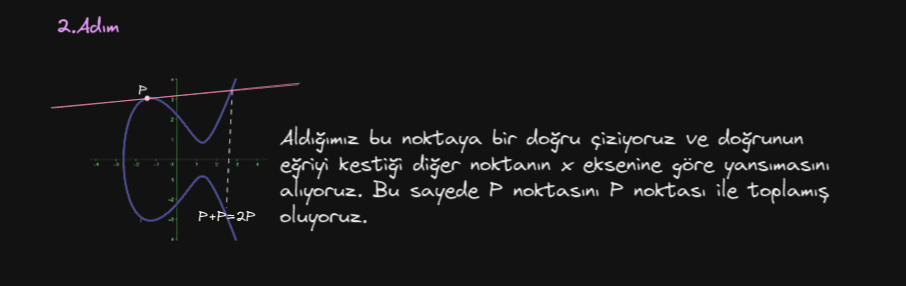


Gitgide blockchainde eliptik eğrinin görevine yaklaşıyoruz ama son bir adım kaldı. Yukarıdaki floodlarda 2 farklı noktanın toplanmasını görmüştük. Peki bir nokta kendisi ile nasıl toplanır?+++

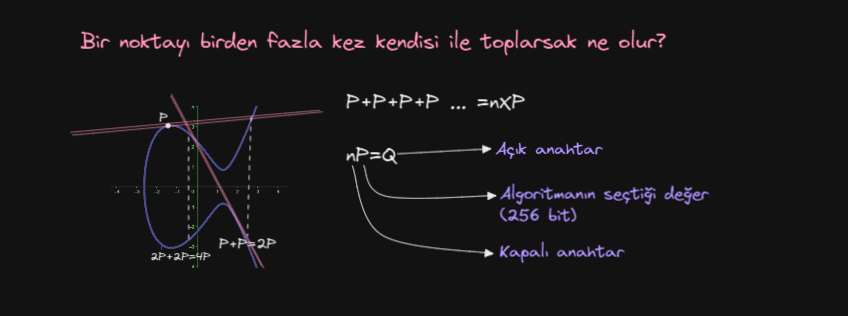
İlk adım olarak eliptik eğri üzerinden bir nokta seçiyoruz.+++



İkinci adımda ise bu noktaya teğet olan bir doğru seçiyoruz. Bu doğru eğriyi herhangi bir 2. Noktada kesmeli. Ardından kesilen noktanın tekrardan x eksenine göre yansımasını alıyoruz. Bu kadar 😊 +++



Bu işlem, bizim cüzdan adreslerimizin şifrelenmesinin ilk adımlarından biri."Bunun dışında kriptoloji ile eliptik eğri nasıl bağlanıyor?" sorusunun da cevabı,bu kısımdan sonra başlıyor. Devam edelim..

Bir sayıyı birden fazla kez eliptik eğri üzerinde toplarsak ne olur? Cevabı aşağıda:Burada gördüğümüz üzere herhangi bir P noktası için n kez toplama işlemi yapılması sonucunda karşımıza Q açık anahtarı çıkmakta. +++

İşte hazırız. Bir veri eliptik eğri üzerinde şifreleme işlemine tabi tutulurken aşağıdaki adımları teker teker uyguluyoruz.  
