8. Eliptik Eğri Çarpanlara Ayırma Metodu

Eliptik eğri çarpanlara ayırma metodu $(p-1)$ algoritmasındaki düşünceyi kullandığından öncelikle $(p-1)$ metodunu inceleyelim.

$p-1$ **Algoritması** :

Eğer $p-1$ büyük asal bölenlere sahip değilse, bu algoritma verilen bir n tamsayısının p asal bölenini genellikle bulur.

1. Gir B, n (B üst sınır)
2. $1 \leqslant a \leqslant n-1$ olacak şekilde rasgele bir a tamsayısı seç
3. $k = 2, 3, ..., B$

   $a := a^k \pmod n$
4. $d := ebob(a-1, n)$
5. Eğer $d = 1$ veya n ise git Adım 2, Aksi halde $p := d$ ve Bitir.

Şimdi algoritmanın nasıl çalıştığını anlatalım. Kabul edelim ki $p-1$ sayısını bölen bütün asal üsler B üst sınırından daha küçük olsun. $B!$, B den küçük sayıların hepsini böldüğünden $p-1 \mid B!$ dir. Fermat teoreminden

$$a^{p-1} \equiv 1 \pmod p$$

dir.

$$a^{p-1} \equiv 1 \pmod p \text{ ve } p-1 \mid B! \Longrightarrow a^{B!} \equiv 1 \pmod p$$

$$a^{B!} \equiv 1 \pmod p \Longrightarrow p \mid ebob(a^{B!}-1, n)$$

Sonuç olarak, eğer $ebob(a^{B!}-1,n) \neq 1$ ve n ise $ebob(a^{B!}-1,n) = p$ olur ve n sayısının bir asal bölenini bulmuş oluruz. $p-1$, $\mathbb{Z}_p$ deki terslenebilen elemanların sayısıdır. Eliptik eğri çarpanlara ayırma metodunda $p-1$ in burada üstlendiği benzer rolü $\mathbb{Z}_p$ üzerindeki eliptik eğrinin eleman sayısı üstlenecek.

n asal olmasın. **Bölüm 5.5** de $\mathbb{F}_q$ ($q = p^r$, p asal) sonlu cisim üzerindeki eliptik eğriler için tanımladığımız toplama kuralını $\mathbb{Z}_n$ için de aşağıdaki gibi tanımlayalım. $\mathbb{Z}_n$ üzerinde tanımlı $y^2 = x^3 + ax + b$ denklemli eliptik eğriyi E ile gösterelim.

$P = (x_1, y_1)$ ve $Q = (x_2, y_2)$ eliptik eğri üzerindeki herhangi iki nokta olsun:

(1) Eğer $y_1 \equiv 0 \pmod{n}$ ise $P := -P$ ve $P + P := \vartheta$

(2) Eğer $x_2 \equiv x_1 \pmod{n}$ ve $y_2 \equiv -y_1 \pmod{n}$ ise $P + Q := \vartheta$

(3) Diğer durumlarda, $P + Q = (x_3, y_3)$ olsun.

Eğer $P = Q$ ise

$$m := (y_2 - y_1)(x_2 - x_1)^{-1} \pmod{n} \tag{8.1}$$

Aksi halde;

$$m := (3x_1^2 + a)(2y_1)^{-1} \pmod{n} \tag{8.2.}$$

olmak üzere

$$x_3 := (m^2 - x_1 - x_2\,) \pmod{n} \qquad \text{ve} \qquad y_3 := (m(x_1 - x_3) - y_1) \pmod{n} \text{ dir.}$$

E eliptik eğrisi üzerinde P ve Q noktalarının toplamı için aşağıdaki üç durum vardır.

1. Durum : Toplam sonsuzdaki noktadır.

2. Durum : (8.1) ve (8.2.) denklemlerinde $ebob(x_2-x_1, n) = 1$ veya $ebob(y_1, n) = 1$ ise toplama kuralı tanımlıdır ve $P + Q := (x_3, y_3)$ dür.

3. Durum : (8.1) ve (8.2.) denklemlerinde $x_2 - x_1$ veya y_1 Modül n ye göre terslenemez ise $P + Q$ toplamı tanımsızdır.

3. Durumdan dolayı E eliptik eğrisi bir grup oluşturmaz. Bu durumu biraz daha inceleyelim.

(8.1) denkleminde eğer x_2-x_1 Modül n e göre terslenemez ise $ebob(x_2-x_1, n) > 1$ dir. Eğer $ebob(x_2 - x_1, n) \neq n$ ise $ebob(x_2 - x_1, n)$, n tamsayısının 1 ve n den farklı bir bölenidir.

Aynı şekilde (8.2.) denkleminde y_1 Modül n e göre terlenemezse $ebob(y_1, n) > 1$ dir. Ve $ebob(y_1, n) \neq n$ ise $ebob(y_1, n)$, n tamsayısının 1 ve n den farklı bir bölenidir. Sonuç olarak, E eliptik eğrisi üzerinde bir P noktası ve büyük bir k tamsayısı için kP skaler çarpımını hesaplarken 3. Durum gerçekleştiğinde toplama işlemini yapamayız. Fakat bu durumla karşılaştığımızda zaten n sayısının bir bölenini bulmuş oluruz.

Şimdi, Eliptik eğri kullanmamızın faydasını görelim. Kabul edelim ki p asalı n sayısının bir böleni olsun. E_p üzerinde tanımlanan $y^2 = x^3+ax+b$ denklemli eğriyi $\overline{E}$ ile gösterelim. $\overline{E}$ eliptik eğrisinin değişmeli bir grup olduğunu biliyoruz. $P \in E$ noktasının Modül p ye indirgenmiş halini $\overline{P}$ noktası ile gösterelim. $\overline{kP} = k\overline{P}$ dir.

$\left|\overline{E}\right|$, $\overline{E}$ eliptik eğrisi üzerindeki nokta sayısını göstersin. $\left|\overline{E}\right| \mid k$ olduğunda $k\overline{P} = \vartheta$ dır. kP skaler çarpımını hesaplarken $\left|\overline{E}\right| \mid k$ durumunda $k\overline{P} = \vartheta$ olduğundan $x_2 - x_1 \equiv 0 \pmod{p}$ olur.

$$p \mid n \text{ ve } p \mid x_2 - x_1 \Longrightarrow ebob(x_2 - x_1, n) > 1$$

Böylece, $ebob(x_2 - x_1, n)$ sayısı n nin bir bölenidir. $\left|\overline{E}\right|$ si küçük asal bölenlere sahip olan bir çok eliptik eğri olduğundan eliptik eğri metodu $p-1$ metodundan daha etkilidir.

Algoritma 8.1. (**Eliptik eğri çarpanlara ayırma algoritması**)

Bu algoritma verilen bir n sayısının bir bölenini bulur.

1. T ilk m asaldan oluşan bir dizi olsun.

2. $a := 1$

3. $P = (0, 1)$

4. $i := 1$

5. $E := y^2 = x^3 + ax + 1$

6. Eğer $i \leqslant m$ ise $k := T[i]$, aksi halde $a := a + 1$ ve Git adım 3

7. $P := kP$ yi hesapla. Eğer hesaplama başarısız (toplama tanımsız) ise Git adım 8, aksi halde $i := i + 1$ ve Git adım 6

8. Eğer n sayısının bir böleni bulunduysa böleni yaz ve Bitir , aksi halde $a := a + 1$ ve Git adım 3

Örnek 8.1. $n = 357564082969$ sayısının **Algoritma 8.1** i kullanarak bir bölenini bulalım. T dizisi ilk 100 asaldan oluşsun. Algoritma $y^2 = x^3 + x + 1$ ve

$y^2 = x^3 + 2x + 1$ denklemli eliptik eğriler için n sayısının asal bölenini bulamaz. $y^2 = x^3 + 3x + 1$ denklemli eğride $P = (0, 1)$ noktası için $(149.139....5.3.2)P$ noktasını hesaplarken

$$(269927330530, 348260288613) + (269927330530, 348260288613)$$

toplamı tanımsızdır. Yani, 348260288613 sayısının Modül n de tersi yoktur. Sonuç olarak, n sayısının bir böleni

$$ebob(348260288613, n) = 430811 \text{ dir.}$$