Kapak Konusu: Modüler ve p-sel Sayılar

Hensel Önsavı

Bu yazıda İmkânsızı Başarmaya Çalışmak adlı yazımızda yapmaya çalıştığımızı daha teorik bir düzeyde yapacağız. Ama bu yazı o yazı okunmadan da anlaşılabilir, o yazıdan bağımsızdır.

Okura ilginç geleceğini umduğumuz iki örnekle başlayalım yazıya.

Örnek 1. $x^2 \equiv 2 \pmod{7^n}$ denkliğini her n için olmasa da birkaç n için çözmeye çalışalım.

Eğer $n = 1$ ise, $a_1 = 3$ ve $b_1 = 4$ bu denkliğin iki çözümüdür. Bunu kontrol etmesi kolaydır.

Deneme yanılma yoluyla (hesaplar uzun olabilir), $a_2 = 10$ ve $b_2 = 39$, $x^2 = 2 \pmod{7^2}$ denkliğin iki çözümüdür ve başka da çözüm yoktur. Burada,

$$a_2 \equiv a_1 \pmod 7 \text{ ve } b_2 \equiv b_1 \pmod 7$$

denkliklerine dikkatinizi çekerim.

Gene deneme yanılma yoluyla, $n = 3$ için de çözümleri bulabiliriz. Bu kez hesaplar biraz daha zaman alır, ama atla deve değildir, birkaç saat içinde kolaylıkla çözümler bulunur: $a_3 = 108$ ve $b_3 = 235$ $x^2 = 2 \pmod{7^3}$ denkliğinin çözümüdür ve başka da çözüm yoktur. Burada da, yukarda olduğu gibi,

$$a_3 \equiv a_2 \pmod{7^2} \text{ ve } b_3 \equiv b_2 \pmod{7^2}$$

denkliklerine dikkatinizi çekerim.

Bir adım daha giderek $n = 4$ için de çözümleri bulabiliriz: $a_4 = 2166$ ve $b_4 = 235$ (gene!), $x^2 = 2 \pmod{7^4}$ denkliğinin çözümüdür ve başka da çözüm yoktur. Burada da, daha önce olduğu gibi,

$$a_4 \equiv a_3 \pmod{7^3} \text{ ve } b_4 \equiv b_3 \pmod{7^3}$$

denkliklerine gene dikkatinizi çekerim.

Tahmin edileceği üzere $x^2 \equiv 2 \pmod{7^n}$ denkliğinin her zaman iki çözümü vardır (birazdan bunu kanıtlayacağız.) Eğer bu çözümlere a_n ve b_n dersek, o zaman (gerekirse a_n ve b_n'nin yerlerini değiştirerek),

$$a_n \equiv a_{n-1} \pmod{7^{n-1}} \text{ ve } b_n \equiv b_{n-1} \pmod{7^{n-1}}$$

denklikleri sağlanır (bunu da birazdan kanıtlayacağız.) Yani n için bulunan çözümler, n–1 için bulunan çözümlerin bir anlamda devamlarıdır. Örneğin, yukarda bulduğumuz

$$a_4 = 2166 \text{ ve } b_4 = 235$$

$$a_3 = 108 \text{ ve } b_3 = 235$$
$$a_2 = 10 \text{ ve } b_2 = 39$$
$$a_1 = 3 \text{ ve } b_1 = 4$$

çözümleri arasında şöyle bir ilişki vardır:

$$\begin{aligned} a_4 = 2166 &= 108 + 6\cdot 7^3 \\ &= 10 + 2\cdot 7^2 + 6\cdot 7^3 \\ &= 3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 \\ b_4 = 235 &= 235 + 0\cdot 7^3 \\ &= 39 + 4\cdot 7^2 + 0\cdot 7^3 \\ &= 4 + 5\cdot 7 + 4\cdot 7^2 + 0\cdot 7^3. \end{aligned}$$

$x^2 \equiv 2 \pmod{7^5}$ denkliğinin a_5 ve b_5 çözümleri, bu yazıda kanıtlayacağımız üzere, 7'den küçük u ve v doğal sayıları için

$$a_5 = 3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 + u\cdot 7^4$$
$$b_5 = 4 + 5\cdot 7 + 4\cdot 7^2 + 0\cdot 7^3 + v\cdot 7^4$$

biçiminde yazılırlar.

Örnek 2. Şimdi modülo 27 karelere bakalım. Bunları aşağıdaki çizelgede bulacaksınız. Sadece 13'e kadar olan sayıları yazdık, 14 ve sonrasına gerek yok, çünkü, örneğin,

$$14 \equiv -13 \pmod{27}$$

ve

$$14^2 \equiv (-13)^2 \equiv 13^2 \pmod{27}.$$

x	x^2
0	0
1	1
2	4
3	9
4	16
5	25
6	9
7	22
8	10
9	0
10	19
11	13
12	9
13	7

Yandaki çizelgede de görüldüğü gibi modülo 27 her sayı bir kare olmuyor. Kare olan sayılar şunlar:

0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25.

Bu sayıların özelliği ne? Hangi sayıların kare olduklarını nasıl hesap yapmadan anlayabiliriz? İşte bu yazıda bu ve benzeri soruları çözmeye çalışacağız.

Bu on bir kareyi üçlük tabanda yazalım (bknz. aşağıdaki çizelge; en soldaki sayılar onluk tabanda, en sağdaki sayılar üçlük tabanda yazılmış.) Ne gözlemliyoruz? Üçlük tabanda yazılmış sayıların birler hanesinde hiç 2 yok, ge-

$$\begin{aligned}
0 &= 0 + 0\cdot 3 + 0\cdot 3^2 = 000 \\
1 &= 1 + 0\cdot 3 + 0\cdot 3^2 = 001 \\
4 &= 1 + 1\cdot 3 + 0\cdot 3^2 = 011 \\
7 &= 1 + 2\cdot 3 + 0\cdot 3^2 = 021 \\
9 &= 0 + 0\cdot 3 + 1\cdot 3^2 = 100 \\
10 &= 1 + 0\cdot 3 + 1\cdot 3^2 = 101 \\
13 &= 1 + 1\cdot 3 + 1\cdot 3^2 = 111 \\
16 &= 1 + 2\cdot 3 + 1\cdot 3^2 = 121 \\
19 &= 1 + 0\cdot 3 + 2\cdot 3^2 = 201 \\
22 &= 1 + 1\cdot 3 + 2\cdot 3^2 = 211 \\
25 &= 1 + 2\cdot 3 + 2\cdot 3^2 = 221
\end{aligned}$$

nellikle 1 var, iki kez de 0. Bu bir rastlantı değil: Eğer bir sayı modülo 27 bir kareyse, o sayı modülo 3 de bir karedir ve 2, modülo 3 bir kare değildir. Dolayısıyla modülo 27 kare olan bir sayı 3'e bölündüğünde kalan (yani üçlük tabanda yazılımının birler hanesi) ya 0 ya da 1 olmalıdır.

Bir başka önemli gözlem daha: Üçlük tabanda birler hanesi 1 olan her sayı (001, 011, 021, 101, 111, 121, 221) modülo 27 bir karedir.

Yazımızın ilk kısmında, $p \neq 2$ bir asal sayı ve $k \geq 1$ bir doğal sayı olduğunda, hangi sayıların modülo p^k bir kare olduğunu bulacağız. ($p = 2$ iken kareleri bulmak daha zordur, biraz değişik bir yöntem izlemek gerekir; bir başka sayımızda ele alırız bu durumu; şimdilik sayfa 46'daki bilgiyle yetinelim). İkinci kısımda, birinci kısımdaki yöntemi genelleştirip Hensel Önsavı adıyla bilinen önemli bir teorem kanıtlayacağız. Hensel Önsavı hem cebirde hem analizde çok önemlidir ve hâlâ bugün üzerine araştırmalar yapılan, sürekli genelleştirilen bir teoremdir.

İlk teoremimizi yazalım.

Teorem. *$p \neq 2$ bir asal sayı ve $k \geq 1$ bir doğal sayı olsun. p'ye bölünmeyen bir a sayısının modülo p^k bir kare olması için yeter ve gerek koşul, a'nın modülo p bir kare olmasıdır.*

Demek ki teoreme göre modülo p kareleri bildiğimizde, p'ye bölünmeyen hangi sayıların modülo p^k kare olduklarını da bilebiliriz.

Alıştırma. Modülo p kare olan tüm tamsayıları bulun. (**Akıl:** Denemeyin bile, çok zordur, bir başka sayıda görürüz bunu.)

Teoremi kanıtlamadan önce teoremin bir uygulamasını yapalım. $p = 5$ olsun. Yandaki dizelgede gösterildiği gibi, sadece 1 ve 4, yani sadece 1 ve -1 modülo 5 bir karedir. Modülo 5^k bir kare olup da 5'e bölünmeyen sayılar, 5'e bölündüklerinde kalanları ya 1 ya da 4 (yani -1) olan sayılardır; bu sayılar da bir s tamsayısı için, $\pm 1 + 5s$ biçiminde yazılırlar, örneğin, $-6, -4, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24, 26, \ldots$ sayıları modülo 5^k karedirler, $k \geq 1$ hangi doğal sayı olursa olsun.

x	x^2
0	0
1	1
2	4
3	4
4	1

Modülo 5 kareler

Teoremin Kanıtı: Önce a'nın modülo p^k bir kare olduğunu varsayalım. (Bu, teoremin kolay kısmı.) Diyelim, belli bir x tamsayısı için,

$$a \equiv x^2 \pmod{p^k}.$$

Demek ki, $a \equiv x^2 \pmod{p}$. Teoremin kolay kısmı kanıtlandı. Şimdi zor kısmına geçelim.

Teoremimizi k üzerinden tümevarımla kanıtlayacağız. Eğer $k = 1$ ise, kanıtlayacak bir şey yok, savın kendisi a'nın modülo p bir kare olduğunu söylüyor. Şimdi $k \geq 1$ olsun ve savın k için doğru olduğunu varsayıp, savı $k + 1$ için kanıtlayalım. Demek ki, varsayıma göre,

$$a \equiv u^2 \pmod{p^k} \qquad (1)$$

denkliğini sağlayan bir u var ve biz,

$$a \equiv v^2 \pmod{p^{k+1}} \qquad (2)$$

denkliğini sağlayan bir v arıyoruz. v'yi, belli bir w için, $u + wp^k$ biçiminde bulacağız (yani modülo p^k için bulunan çözümü bir adım daha p^{k+1} için devam ettireceğiz): (1)'in doğru olduğunu biliyoruz (daha doğrusu varsayıyoruz) ve (2)'yi ve

$$v = u + wp^k \qquad (3)$$

denklemini sağlayacak bir w (ve v) arıyoruz. Hatta w'yi p'den küçük bir doğal sayı olarak alabileceğiz. Önce, (2) ve (3)'ü sağlayan bir w'nin, eğer varsa neye eşit olması gerektiğini bulacağız, sonra bulduğumuz bu w'nin gerçekten istediğimiz (2) ve (3) denklemlerini sağladığını kanıtlayacağız.

(1)'den dolayı, belli bir t tamsayısı için,

$$a = u^2 + tp^k \qquad (4)$$

eşitliği sağlanır. Şimdi modülo p^{k+1} hesaplayalım:

$$u^2 + tp^k =^{(4)} a \equiv^{(2)} v^2 =^{(3)} (u + wp^k)^2$$
$$= u^2 + 2uwp^k + w^2p^{2k} \pmod{p^{k+1}}.$$

Her iki taraftan da u^2'leri temizleyecek olursak,

$$tp^k \equiv 2uwp^k + w^2p^{2k} \pmod{p^{k+1}}$$

bulunur. Bundan da, p^k'leri temizleyerek,

$$t \equiv 2uw + w^2p^k \pmod{p}$$

bulunur. $k \geq 1$ olduğundan, bu son denklemden,

$$t \equiv 2uw \pmod{p} \qquad (5)$$

çıkar. Şimdi p asalının 2 olmadığını kullanacağız. u, p'ye bölünmediğinden (yoksa, (1) denkleminden a'nın p'ye bölündüğü çıkardı), $2u$ sayısı p'ye asaldır. Demek ki bir s tamsayısı için,

$$2us \equiv 1 \pmod{p} \qquad (6)$$

eşitliği sağlanır [sayfa 33'teki Fermat'nın Küçük Teoremi'ne göre s'yi $(2u)^{p-2}$ alabiliriz]. Şimdi (5)'in her iki tarafını da s'yle çarparak ve (6)'yı kullanarak,

$$w \equiv 1w \equiv^{(6)} 2usw \equiv^{(5)} st \pmod{p} \qquad (7)$$

buluruz. w'yi bulduk galiba, w, st'ye eşit olabilir, hatta w'yi (7)'yi sağlayan p'den küçük bir doğal sayı olarak da alabileceğimizi göreceğiz.

Şimdi sağlamasını yapalım, bakalım w'yi (modülo p ya da değil) st'ye eşit alırsak istediğimiz oluyor mu?

Bildiklerimizi anımsatalım: a verilmiş, p, a'yı bölmeyen ve 2'ye eşit olmayan bir asal.

$$a \equiv u^2 \pmod{p^k} \quad (1)$$

denkliğini sağlayan bir u var (tümevarım varsayımı). Bunları biliyoruz ve,

$$a \equiv v^2 \pmod{p^{k+1}} \quad (2)$$

denkliğini sağlayan bir v arıyoruz.

(1)'den dolayı, belli bir t tamsayısı için,

$$a = u^2 + tp^k \quad (4)$$

eşitliği sağlanır. Gene (1)'den dolayı p, u'yu bölemez. Demek ki p, $2u$'yu da bölmüyor. Dolayısıyla, bir s tamsayısı için ($s = (2u)^{p-2}$ alabilir),

$$2us \equiv 1 \pmod{p} \quad (6)$$

eşitliği sağlanır. Şimdi

$$v = u + stp^k \quad (3)$$

olsun. Bu v'nin (2) denkliğini sağladığını kanıtlayacağız. $2k \geq k + 1$ kullanarak hesaplayalım:

$$v^2 =^{(3)} (u + stp^k)^2 = u^2 + 2ustp^k + s^2t^2p^{2k}$$
$$\equiv u^2 + 2ustp^k \equiv^{(6)} u^2 + tp^k =^{(4)} a \pmod{p^{k+1}}.$$

Dilediğimiz gibi bir v bulduk ve böylece teoremimiz kanıtlanmış oldu. □

Yukardaki kanıt eğer dikkatlice incelenirse şu anlaşılır:

Sonuç. *Eğer* $x_0 = 1, 2, ..., p-1$ *sayısı,*

$$a \equiv x_0^2 \pmod{p}$$

denkliğini sağlıyorsa, o zaman öyle $x_1, x_2, ..., x_k \in \{0, 1, ..., p-1\}$ *sayıları vardır ki,*

$$a \equiv (x_0 + x_1p + ... + x_{k-1}p^{k-1})^2 \pmod{p^k}$$

denkliği sağlanır, yani öyle bir x tamsayısı vardır ki, her $i = 1, 2, ..., k$ *için,* $a \equiv x^2 \pmod{p^i}$.

Şimdi bu kanıtın yöntemini kullanarak yukardakinden çok daha genel bir teorem kanıtlayacağız.

Önce bir tanım (ya da anımsatma): Eğer

$$f(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

bir polinomsa, bu polinomun ***türevi*** $f'(X)$ şöyle tanımlanır:

$$f'(X) = a_1 + 2a_2X + 3a_3X^2 + ... + na_nX^{n-1}.$$

Teorem (Hensel Önsavı). $f(X) \in \mathbb{Z}[X]$ *bir polinom olsun. Eğer,*

$$f(x_0) \equiv 0 \pmod{p}$$

ve

$$f'(x_0) \not\equiv 0 \pmod{p}$$

koşullarını sağlayan bir $x_0 \in \mathbb{Z}$ *varsa, o zaman her k pozitif doğal sayısı için,*

$$f(x) \equiv 0 \pmod{p^k}$$

ve

$$x \equiv x_0 \pmod{p}$$

denkliklerini sağlayan bir x vardır ve bu x, modülo p^k *bir tanedir.*

Kanıt: Önce x'in varlığını kanıtlayacağız, x'in modülo p^k biricikliğine daha sonra sıra gelecek. Bunu k üzerine tümevarımla kanıtlayacağız. Eğer $k = 1$ ise kanıtlayacak bir şey yok, bu durumda teorem, varsayımın kendisi: x'i x_0 almak yeterli. Şimdi x'in varlığını pozitif bir k tamsayısı için varsayıp, $k + 1$ için kanıtlayalım. $x \in \mathbb{Z}$,

$$f(x) \equiv 0 \pmod{p^k} \quad (8)$$

ve

$$x \equiv x_0 \pmod{p} \quad (9)$$

denkliklerini sağlasın (tümevarım varsayımı).

$$f(y) \equiv 0 \pmod{p^{k+1}} \quad (10)$$

ve

$$y \equiv x_0 \pmod{p} \quad (11)$$

denkliklerini sağlayan bir y arıyoruz. Aradığımız y'yi belli bir z için,

$$y = x + p^kz \quad (12)$$

biçiminde bulacağız, yani modülo p^{k+1} çözüm, modülo p^k çözümü bir adım daha devam ettirecek, aynen bir üstteki teoremin kanıtındaki gibi. Ayrıca z'yi p'den küçük bir doğal sayı olarak alabileceğimizi de göreceğiz.

f polinomunu açık bir biçimde yazalım:

$$f(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

olsun, yani

$$f(X) = \sum_i a_iX^i$$

olsun.

Daha önceki teoremin kanıtında da yaptığımız gibi, önce, (8-12) koşullarını sağlayan bir z'nin ne olabileceğini bulacağız. Daha sonra bu olası çözüm z'yi (12)'ye yerleştirdiğimizde, y'nin gerçekten (10) koşulunu sağladığını kanıtlayacağız. (12) eşitliği sağlanmış olacağından, (9)'dan dolayı (11) kendiliğinden sağlanacak.

Başlıyoruz. Dediğimiz gibi, (8-12)'yi varsayıp z'nin alabileceği değeri bulacağız. Modülo p^{k+1} hesaplayalım:

$$0 \equiv f(y) = f(x + p^kz) = \sum_i a_i(x + p^kz)^i$$
$$= \sum_i (a_ix^i + ip^kza_ix^{i-1} + ...) \pmod{p^{k+1}}.$$

Toplamanın altındaki "nokta nokta"larda p^{2k}, p^{3k} gibi p'nin $k+1$'den büyük güçleri var. Dolayısıyla modülo p^{k+1} alınınca kaybolurlar ve geriye

$$0 \equiv \sum_i (a_i x^i + ip^k z a_i x^{i-1}) \pmod{p^{k+1}}.$$

kalır. Hesaba devam edelim:

$$\begin{aligned} 0 &\equiv \sum_i (a_i x^i + ip^k z a_i x^{i-1}) \\ &\equiv \sum_i a_i x^i + p^k z \sum_i i a_i x^{i-1} \\ &= f(x) + p^k z f'(x) \pmod{p^{k+1}}. \end{aligned}$$

(8)'e göre, bir t tamsayısı için,

$$f(x) = p^k t \tag{13}$$

eşitliği geçerlidir. Bunu bir önceki denkleme yerleştirirsek,

$$0 \equiv p^k t + p^k z f'(x) \pmod{p^{k+1}}$$

buluruz. Sadeleştirmeyle,

$$0 \equiv t + z f'(x) \pmod{p} \tag{14}$$

elde ederiz. Şimdi, $f'(x) \not\equiv 0 \pmod{p}$ koşulunu kullanarak, (14)'ü sağlayan bir z buluruz, hatta z'yi p'den küçük bir doğal sayı bile seçebiliriz: Eğer

$$sf'(x) \equiv 1 \pmod{p} \tag{15}$$

ise z'yi,

$$z \equiv -ts \pmod{p} \tag{16}$$

olacak biçimde seçelim. Dilersek z'yi $-ts$'ye eşit seçebileceğimiz gibi, (16)'yı sağlayan herhangi bir tamsayı olarak da seçebiliriz, örneğin, z'yi p'den küçük bir doğal sayı olarak seçebiliriz. Şimdi bulduğumuz bu z'nin gerçekten istediğimiz denkliği sağladığını kanıtlayalım.

Hikâyemizi ta başından anımsatalım: $x \in \mathbb{Z}$,

$$f(x) \equiv 0 \pmod{p^k} \tag{8}$$

denklemini sağlıyor, ama

$$f'(x) \not\equiv 0 \pmod{p}. \tag{17}$$

Bunlar tümevarım varsayımları. (8)'den dolayı,

$$f(x) = p^k t \tag{13}$$

eşitliğini sağlayan bir t tamsayısı vardır. (17)'den dolayı,

$$sf'(x) \equiv 1 \pmod{p}$$

denkliğini sağlayan bir s tamsayısı vardır. Demek ki,

$$sf'(x) = 1 + pm \tag{15}$$

eşitliğini sağlayan bir m tamsayısı da vardır. Şimdi, z,

$$z \equiv -ts \pmod{p}$$

denkliğini sağlayan herhangi bir tamsayı olsun, yani bir r tamsayısı için,

$$z = -ts + pr \tag{16}$$

eşitliği sağlansın. Dilersek z'yi $p-1$'den küçük bir doğal sayı olarak da seçebiliriz. Şimdi, y,

$$y = x + p^k z \tag{12}$$

olarak tanımlansın. Yukardaki eşitlik ve denklikler ışığında

$$f(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n = \sum_i a_i X^i$$

polinomunun y'de aldığı $f(y)$ değerini modülo p^{k+1} hesaplayalım (yukarda yaptığımız hesapları tekrar yapacağız):

$$\begin{aligned} f(y) &= f(x + p^k z) && \text{(12)'den} \\ &= \sum_i a_i (x + p^k z)^i && f\text{'nin tanımı} \\ &= \sum_i a_i (x^i + ip^k z x^{i-1} + \ldots) && \text{hesap} \\ &\equiv \sum_i (a_i x^i + ip^k z a_i x^{i-1}) && 2k \geq k+1 \\ &= \sum_i a_i x^i + p^k z \sum_i i a_i x^{i-1}) && \text{hesap} \\ &= f(x) + p^k z f'(x) && f \text{ ve } f' \text{ in tanımı} \\ &= p^k t + p^k z f'(x) && \text{(13)'ten} \\ &= p^k t + p^k (-ts + pr) f'(x) && \text{(16)'dan} \\ &\equiv p^k t - p^k ts f'(x) && \pmod{p^{k+1}} \\ &\equiv p^k t - p^k t(1 + pm) && \text{(15)'ten} \\ &\equiv 0 && \pmod{p^{k+1}} \end{aligned}$$

Teoremimizin yarısı kanıtlanmıştır.

Şimdi, f'nin bulduğumuz bu kökünün modülo p^k biricikliğini kanıtlayalım.

$$f(x_0) \equiv 0 \pmod{p} \text{ ve } f'(x_0) \not\equiv 0 \pmod{p}$$

koşullarını sağlayan bir $x_0 \in \mathbb{Z}$ olsun.

$$f(x) \equiv f(y) \equiv 0 \pmod{p^k}$$

ve

$$x \equiv y \equiv x_0 \pmod{p}$$

denkliklerini sağlayan x ve y olsun.

$$x \equiv y \pmod{p^k}$$

denkliğini kanıtlayacağız. Bunu k üzerine tümevarımla yapacağız. $k = 1$ ise kanıtlayacak bir şey yok.

$$x \equiv y \pmod{p^{k-1}}$$

denkliğini varsayalım. Demek ki, bir z tamsayısı için, $y = x + p^{k-1}z$ eşitliği geçerli. z'nin p'ye bölündüğünü kanıtlamalıyız. Modulo p^k hesaplayalım:

$$\begin{aligned} 0 &\equiv f(y) \equiv f(x + p^{k-1}z) \equiv f(x) + p^{k-1} z f'(x) \\ &\equiv p^{k-1} z f'(x) \pmod{p^k}. \end{aligned}$$

(En sondan bir önceki denklikte daha önce yaptığımız gibi hesapladık.) Ama $f'(x) \not\equiv 0 \pmod{p}$ olduğundan, bundan $0 \equiv p^{k-1}z \pmod{p^k}$, yani $z \equiv 0 \pmod{p}$ bulunur. Teoremimiz kanıtlanmıştır. □

Yukardaki teoremi p-sel sayılar halkası $\mathbb{Z}_p$'ye de uygulayabiliriz. Hatta f polinomunu $\mathbb{Z}[X]$'te almak yerine $\mathbb{Z}_p[X]$'ten de alabiliriz. Kanıt değişmez.

Teorem ($\mathbb{Z}_p$'de Hensel Önsavı). *$f(X) \in \mathbb{Z}_p[X]$ bir polinom olsun. Eğer*

$$f(x_0) \equiv 0 \pmod{p}$$

ve

$$f'(x_0) \not\equiv 0 \pmod{p}$$

koşullarını sağlayan bir $x_0 \in \mathbb{Z}$ (ya da $x_0 \in \mathbb{Z}_p$, farketmez) varsa, o zaman

$$f(x) \equiv 0 \pmod{p^k} \text{ ve } x \equiv x_0 \pmod{p}$$

denkliklerini sağlayan bir ve bir tek $x \in \mathbb{Z}_p$ vardır. ♦