Cahit Arf Matematik Günleri 10
2. Aşama Sınavı

30 Nisan 2011
Süre: 8 saat

Notasyon:
$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ (doğal sayılar)
$\mathbb{C} = \{a + bi \colon a, b \text{ gerçel sayı}\}$ (karmaşık sayılar)
$\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ (asal sayılar)
$\mathbb{P}_{a,b} = \{p \in \mathbb{P} \colon p \equiv a \mod b\}$
f, tamsayı katsayılı bir polinom olmak üzere

$$\mathbb{P}_f = \{p \in \mathbb{P} \colon \text{bir } n \in \mathbb{N} \text{ için } p \mid f(n)\}$$

1. $\mathbb{P}$ kümesinin sonsuz olduğunu kanıtlayın. (5 puan)

   Çözüm: Diyelim ki sonlu sayıda asal var. O zaman tüm asalları $p_1, \ldots, p_k$ şeklinde sıralayabiliriz. $n = p_1 \cdots p_k + 1$ olsun. Elbette n sayısı 1'den büyük ve dolayısıyla n'yi bölen bir p asalı var. Diğer yandan, $p_1, \ldots, p_k$ tüm asal sayıların bir listesi olduğundan, bir i için $p = p_i$ olmalı. Ama n'nin herhangi bir p_i'ye bölümünden kalan 1. Çelişki.

2. $\mathbb{P}_{3,4}$ kümesinin sonsuz olduğunu kanıtlayın. (10 puan)

   Çözüm: Diyelim ki $\mathbb{P}_{3,4}$ kümesi sonlu. O zaman $\mathbb{P}_{3,4}$ kümesinin tüm elemanlarını $p_1, \ldots, p_k$ şeklinde sıralayabiliriz. $n = 4p_1 \cdots p_k - 1$ olsun. Elbette n sayısı tek ve 1'den büyük. Dolayısıyla n, tek asal sayıların çarpımı olarak yazılabiliyor. Eğer n'nin tüm asal bölenleri $\mathbb{P}_{1,4}$ kümesinde olsaydı n sayısı mod 4'te 1'e denk olurdu. Demek ki n sayısınının $\mathbb{P}_{3,4}$ kümesinden bir p böleni olmalı. Diğer yandan, $\mathbb{P}_{3,4}$ kümesindeki tüm sayılar $p_1, \ldots, p_k$ listesinde olduğundan, bir i için $p = p_i$ olmalı. Ama n'nin herhangi bir p_i'ye bölümünden kalan $p_i - 1$. Çelişki.

3. Eğer f sabit değilse $\mathbb{P}_f$ kümesinin sonsuz olduğunu kanıtlayın. (15 puan)

   Çözüm: Eğer f polinomunun sabit terimi sıfırsa, tamsayı katsayılı bir g polinomu için $f(x) = xg(x)$ sağlanır. Buradan da, $n \mid f(n)$ olduğu için, $\mathbb{P}_f = \mathbb{P}$ çıkar. Yani f'nin sabit teriminin sıfır olmadığını varsayabiliriz. $f(x)$ polinomunu

   $$f(x) = \sum_{i=0}^{d} a_i x^i$$

   olarak yazalım. Elbette $a_0 \neq 0$, $d > 0$ ve $a_0, \ldots, a_d$ tamsayı. Diyelim ki $\mathbb{P}_f$ kümesi sonlu. O zaman $\mathbb{P}_f$ kümesinin tüm elemanlarını $p_1, \ldots, p_k$

şeklinde sıralayabiliriz. Şimdi $n_t = f(a_0 p_1^t \cdots p_n^t)$ ve $m_t = n_t/a_0$ olsun. Bu durumda,

$$n_t = \sum_{i=0}^{d} a_i a_0^i p_1^{it} \cdots p_k^{it} = a_0 \left(1 + \sum_{i=1}^{d} a_i a_0^{i-1} p_1^{it} \cdots p_k^{it}\right) = a_0 m_t$$

eşitliği yüzünden, eğer t yeterince büyükse, m_t, 1'den büyük olur. Dolayısyla m_t'nin asal bir p böleni vardır. Elbette p asalı n_t'yi de böler, yani p, $\mathbb{P}_f$'dedir. Buradan da bir i için $p = p_i$ olduğu çıkar. Ama m_t'nin herhangi bir p_i'ye bölümünden kalan 1. Çelişki.

4. $\mathbb{P}_{1,4}$ kümesinin sonsuz olduğunu kanıtlayın. (20 puan)

   Çözüm: $f(x) = x^2+1$ olsun. 3 numaralı sorudan $\mathbb{P}_f$ sonsuz. Eğer $\mathbb{P}_f \cap \mathbb{P}_{3,4}$ kümesinin boş olduğunu gösterirsek $\mathbb{P}_{1,4}$ kümesinin sonsuz olduğu çıkar, çünkü $\mathbb{P} = \mathbb{P}_{1,4} \cup \{2\} \cup \mathbb{P}_{3,4}$.

   Diyelim ki $\mathbb{P}_{3,4}$ kümesinde öyle bir p var ki bir n için $p \mid n^2 + 1$, yani $n^2 \equiv -1 \mod p$. Diğer yandan Fermat'nın küçük teoreminden $n^{p-1} \equiv 1 \mod p$. Bunu, ve $(p-1)/2$ tamsayısının tek oluşunu kullanarak

   $$1 \equiv n^{p-1} \equiv (n^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \mod p$$

   elde ederiz. p tek olduğundan bu mümkün değil.

5. Pozitif bir n tamsayısı için $\zeta_n = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ olsun. Şu polinomu tanımlayalım:

   $$\Phi_n(x) = \prod_{\substack{1 \le d \le n \\ \text{obeb}(n,d)=1}} (x - \zeta_n^d).$$

   (Üç şık toplam 50 puan)

   (a) $\Phi_n(x)$ polinomunun katsayılarının tamsayı olduğunu kanıtlayın.
   Çözüm: De Moivre formülünden[1]

   $$x^n - 1 = \prod_{d=1}^{n} (x - \zeta_n^d)$$

   olduğunu biliyoruz. Buradan hemen $\Phi_n(x) \mid x^n - 1$ olduğu çıkıyor. Şimdi $x^n - 1$ polinomunun köklerini başka bir biçimde ifade edeceğiz. U kümesi 1 in tüm karmaşık köklerinden oluşan küme olsun. Yani

   $$U = \{z \in \mathbb{C} \colon \text{ bir } n \in \mathbb{N} \text{ için } z^n = 1\}.$$

   U kümesi üzerinde şu fonksiyonu tanımlayalım

   $$o(z) = \min\{n \in \mathbb{N} \colon z^n = 1 \text{ ve } n > 0\}.$$

   Tanımladığımız bu o fonksiyonunun temel bazı özelliklerini kanıtlayacağız.

[1] De Moivre formülü her n tamsayısı ve θ gerçel sayısı için $(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$ olduğunu söyler. Tümevarımla kanıtlanabilir.

Diyelim ki $z^n = 1$ ve $n \geq 1$. Bu durumda tanım gereği $o(z) \leq n$. Eğer $a, b \in \mathbb{N}$ ve $b < o(z)$ olacak şekilde $n = o(z)a + b$ yazarsak

$$1 = z^n = z^{o(z)a+b} = (z^{o(z)})^a z^b = z^b$$

elde ederiz. Buradan da $b < o(z)$ olduğundan $b = 0$ çıkar. Yani $o(z) \mid n$. Diğer yandan herhangi bir n için $o(z) \mid n$ ise $z^n = 1$ olur. Bütün bunları

$$x^n - 1 = \prod_{o(\zeta)|n} (x - \zeta)$$

eşitliğiyle özetleyebiliriz. Benzer bir eşitliği $\Phi_n(x)$ için kanıtlamak istiyoruz. İlk önce o fonksiyonunun başka bir karakterizasyonunu görelim. Eğer $\zeta \in U$ ise

$$\langle \zeta \rangle = \{\zeta^n : n \in \mathbb{N}\}$$

olsun. Kolayca görülebileceği gibi $o(\zeta)$ tam olarak $\langle \zeta \rangle$ kümesideki eleman sayısı. Bunu kullanarak $o(\zeta_n^d) = n$ olması için gerekli ve yeterli koşulun $\text{obeb}(d, n) = 1$ olduğunu kanıtlayacağız.

Diyelim ki $\text{obeb}(d, n) = 1$. Bu durumda öyle a, b tamsayıları vardır ki $ad + bn = 1$ olur. Buradan da

$$\zeta_n = \zeta_n^{ad+bn} = (\zeta_n^n)^a (\zeta_n^d)^b = (\zeta_n^d)^b$$

çıkar. Yani $\zeta_n \in \langle \zeta_n^d \rangle$ ve dolayısıyla $\langle \zeta_n \rangle \subseteq \langle \zeta_n^d \rangle$. Öte yandan tanım gereği $\langle \zeta_n^d \rangle \subseteq \langle \zeta_n \rangle$. Demek ki $\langle \zeta_n^d \rangle = \langle \zeta_n \rangle$ ve $o(\zeta_n^d) = o(\zeta_n)$. De Moivre formülünden $o(\zeta_n) = n$ olduğunu görmek kolay.

Şimdi de diyelim ki $\text{obeb}(d, n) = k \neq 1$. Elbette $o(\zeta_n^k) < n$ çünkü $(\zeta_n^k)^{\frac{n}{k}} = 1$. Öte yandan $\zeta_n^d = (\zeta_n^k)^{\frac{d}{k}} \in \langle \zeta_n^k \rangle$. Yani $\langle \zeta_n^d \rangle \subseteq \langle \zeta_n^k \rangle$. Buradan da $o(\zeta_n^d) \leq o(\zeta_n^k) < n$ eşitsizliği çıkar.

Bunlara ek olarak $(\zeta_n^d)^n = 1$, dolayısıyla $o(\zeta_n^d) \mid n$. Tüm bunları şu eşitlikle özetleyebiliriz:

$$\Phi_n(x) = \prod_{o(\zeta)=n} (x - \zeta).$$

Bu da bize $\Phi_n(x)$ için tümevarımsal bir formül veriyor:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d\neq n} \Phi_d(x)}.$$

Bundan sonrası için tümevarım yapacağız. $\Phi_1(x) = x - 1$ ve dolayısıyla tüm katsayıları tamsayı. Diyelim ki n'den küçük her d için $\Phi_n(x)$ polinomu tamsayı katsayılı. Buradan, $\Phi_d(x)$'lerin başat katsayıları 1 olduğu için, $\Phi_n(x)$ polinomunun tamsayı katsayılı olduğu çıkar.

(b) $p \in \mathbb{P}$ ve $a \in \mathbb{N}$ olsun. Diyelim ki p asalı n'yi bölmüyor ama $\Phi_n(a)$'yı bölüyor. Bu durumda $a^n \equiv 1 \mod p$ denkliğinin sağlandığını ve n sayısının bu denkliği sağlayan en küçük pozitif tamsayı olduğunu kanıtlayın.

Çözüm: Bir önceki sorudan

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

olduğunu biliyoruz. Bu eşitlikte $x = a$ alıp eşitliğe mod p'de bakarsak $a^n \equiv 1 \mod p$ olduğunu görürüz. m, $a^m \equiv 1 \mod p$ denkliğini sağlayan en küçük pozitif tamsayı olsun. $0 \leq l < m$ olmak üzere $n = km + l$ yazalım. Bu durumda

$$1 \equiv a^n \equiv a^{km+l} \equiv (a^m)^k a^l \equiv a^l \mod p$$

eşitliğinden $b = 0$ olduğu, yani m'nin n'yi böldüğü çıkar. Yani $\Phi_m(x)$ polinomu $x^n - 1$ polinomunu bölüyor. Diğer yandan

$$x^m - 1 = \prod_{d|m} \Phi_m(x)$$

olduğundan m'yi bölen bir d için $\Phi_d(a) \equiv 0 \mod p$ olmalı. Ama $\Phi_d(x)$ polinomu $x^d - 1$'i bölüyor. Yani $a^d \equiv 1 \mod p$ sağlanmalı. Buradan da m bu özelliği sağlayan en küçük pozitif tamsayı olduğundan $m = d$ olduğunu görüyoruz. Bu da elbette $\Phi_m(a) \equiv 0 \mod p$ demek.
Diyelim ki $m \neq n$. O zaman tamsayı katsayılı bir $p(x)$ polinomu için

$$x^n - 1 = \Phi_n(x)\Phi_m(x)p(x)$$

eşitliği sağlanır. Her iki tarafın türevini alırsak

$$nx^{n-1} = \Phi_n'(x)\Phi_m(x)p(x) + \Phi_n(x)\Phi_m'(x)p(x) + \Phi_n(x)\Phi_m(x)p(x)'$$

elde ederiz. Şimdi bu eştlikte $x = a$ alıp eşitliğe mod p'de bakarsak, $\Phi_n(a) \equiv \Phi_m(a) \equiv 0 \mod p$ olduğundan, $na^{n-1} \equiv 0 \mod p$ elde ederiz. Varsayımımızdan p, n'yi bölmüyor. Demek ki p, a'yı bölüyor. Bu durumda $0 \equiv \Phi_n(a) \equiv \Phi_n(0) \mod p$ olmalı. Ama $\Phi_n(0)$, tanım gereği ζ_n'nin bir kuvveti. Yani $\Phi_n(0)^n = 1$. Diğer yandan $\Phi_n(x)$'in katsayılarının tamsayı olduğunu biliyoruz. Bradan $\Phi_n(0)$'ın ya 1 ya da -1 olduğu çıkıyor. Çelişki, çünkü $\Phi_n(0) \mod p$'de 0. Demek ki $m = n$, başka bir deyişle n, $a^n \equiv 1 \mod p$ denkliğini sağlayan en küçük pozitif tamsayı.

(c) $\mathbb{P}_{1,n}$ kümesinin sonsuz olduğunu kanıtlayın.
Çözüm: 3 numaralı sorudan $\mathbb{P}_{\Phi_n}$ sonsuz. p, $\mathbb{P}_{\Phi_n}$ kümesinde n'yi bölmeyen bir asal olsun. Bir önceki şıktan öyle bir a var ki $a^n \equiv 1 \mod p$ ve eğer $a^k \equiv 1 \mod p$ ise n, k'den küçük. Fermat'nın küçük teoreminden $a^{p-1} \equiv 1 \mod p$. Şimdi $u, v \in \mathbb{N}$ ve $v < n$ olacak şekilde $p - 1 = nu + v$ yazalım. Buradan

$$1 \equiv a^{p-1} \equiv a^{nu+v} \equiv (a^n)^u a^v \equiv a^v \mod p$$

elde ederiz. Ama $v < n$ olduğundan $v = 0$ olduğu, yani n'nin $p - 1$'i böldüğü çıkar. Bu da demek oluyor ki sonsuz bir küme olan $\mathbb{P}_{\Phi_n}$'den n'nin bölenlerini, yani sonlu bir kümeyi çıkarınca $\mathbb{P}_{1,n}$ kümesinin bir altkümesini elde ediyoruz. Yani $\mathbb{P}_{1,n}$ sonsuz.