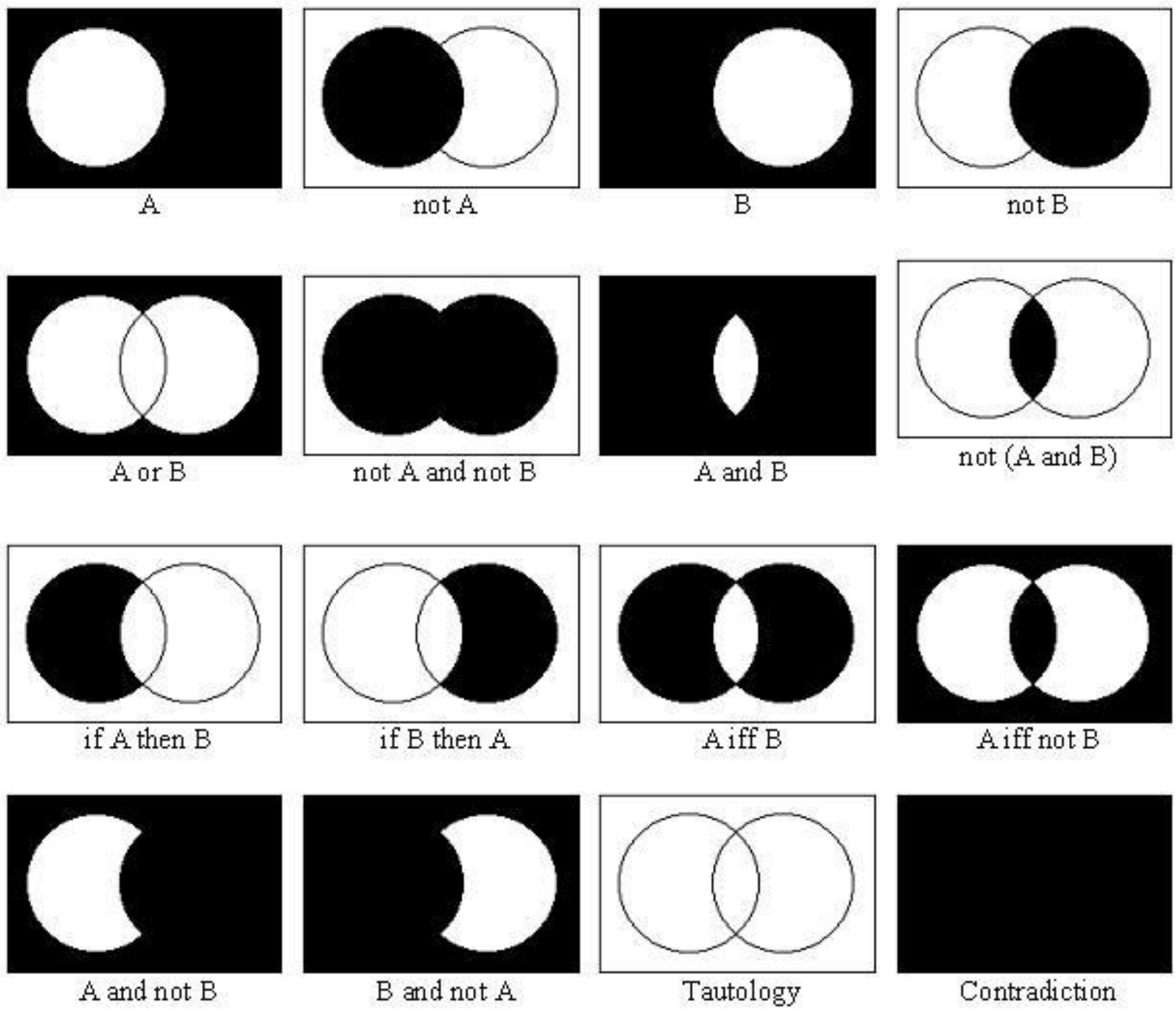
SCHEMES



“The Representation of Logic Compound Propositions by Venn Diagram related to logic slides from page 3 to page 11.”

SOURCE: http://finitegeometry.org/sc/16/venn.html

Premises	Inference	Conclusion
True	Valid	True
		XXXX
	Invalid	True
		False
False	Valid	True
		False
	Invalid	True
		False

“The Table of Validity connected to Proofs Slides page 1-2.”

SOURCE: http://www.philosophypages.com/lg/e01.htm

soru 11

RSA gibi asimetrik şifreleme sistemleri çok büyük asal sayılara ihtiyaç duymaktadır (bkz. UEKAE Dergisi, Sayı: 1, Sayfa: 32-41, "Günümüzde Kriptoloji"). Bu sayıların bulunması için, verilen bir sayının asal olup olmadığını çok yüksek bir doğrulukla (ama kesinlik olmaksızın) belirleyen testler (örneğin Miller-Rabin testi) geliştirilmiştir.

Wilson teoremi diye anılan aşağıdaki teorem bir sayının asal olup olmadığını kesinlikle (yani, hata olasılığı 0 olarak) bulabilmektedir:

> p sayısının asal olması için gerek ve yeter şart:
>
> $$(p\text{-}1)! = \text{-}1 \pmod p$$

(i) Bu teoremin ilk 5 asal sayı için doğru olduğunu gösteriniz.

(ii) Bu teoremi pratikte yukarıda bahsedilen testlerden biri olarak neden kullanamayacağımızı açıklayınız.

“The Question of Prime Numbers related to Number Theory Slides”

SOURCE: BİLGEM Dergisi Sayı 5- sayfa 147,

http://www.uekae.tubitak.gov.tr/uekae_content_files/flash/UEKAE_dergi_sayfa_flash/sayi_5/Default.html

cevap 11

(i) Verilen teorem 2, 3, 5, 7, 11 için doğrudur (gösterim aşağıdadır)

(ii) Çok büyük sayılarla hesaplama gereksinimi dolayısıyla pratikte bu teorem bir asallık testi olarak kullanılamaz.

İlk 5 asal sayı için teoremi deneyelim:

2: (2-1)! = 1! = 1 = -1 (mod 2)

3: (3-1)! = 2! = 2 = -1 (mod 3)

5: (5-1)! = 4! = 24 = -1 (mod 5)

7: (7-1)! = 6! = 720 = -1 (mod 7)

11: (11-1)! = 10! = 3628800 = -1 (mod 11)

Böylece, teoremin ilk 5 asal sayı için doğru olduğu bulunur (bu teoremin ispatı birçok kaynakta mevcuttur, ör. M. R. Schroeder, *Number Theory in Science and Communication*, 3. Ed., Springer, 1997).

Bu teoremi bir asallık testi olarak kullanmak istediğimizi varsayalım, ve RSA benzeri algoritmalar için aslında çok küçük olacak 1000003 sayısı için yukarıdaki deneylerin benzerini uygulamaya çalışalım:

1000003: (1000003-1)! = 1000002! = ? (mod 1000003)

1000002! sayısının ne kadar büyük bir sayı olduğunu görebilmek için, Stirling yakınsama kuralını kullanalım:

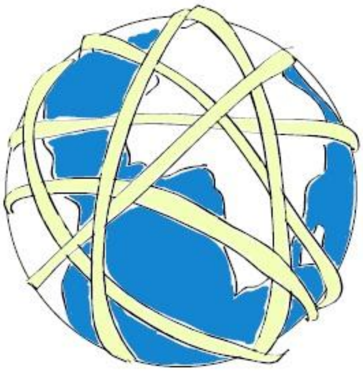
$$1000002! \approx \sqrt{2 \cdot \pi \cdot 1000002} \cdot \left(\frac{1000002}{e}\right)^{1000002} \approx 1,6 \cdot 10^{5565721}$$

Görüyoruz ki, asimetrik şifreleme ölçeğinde çok küçük olan 1000003 sayısının bile asal olup olmadığını bu testle belirlemek için, yukarıdaki 5.565.722 basamaklı sayıyı hesaplamak gerekmektedir. Bu pratik olmadığından, kesin sonuç vermesine rağmen, Wilson teoremi büyük sayılar için asallık testi olarak kullanılamamaktadır.

SOURCE: BİLGEM dergisi 6.sayı-sayfa 173

http://www.uekae.tubitak.gov.tr/uekae_content_files/flash/UEKAE_dergi_sayfa_flash/sayi_5/Default.html

soru 15



Alman matematikçi Georg Cantor (1845-1918), aşağıdaki sanıyı (conjecture) öne sürmüştür:

$$p_0 = 2,\ p_{n+1} = 2^{p_n} - 1$$

kuralına göre oluşturulan tüm p_i, $\forall i$ sayıları asaldır.

(i) p_1, p_2, p_3 sayıları asal mıdır?

(ii) p_5 sayısının on tabanındaki yazılışının yeterli uzunluktaki kağıttan bir şeride (şeridin kalınlığı önemsizdir), bir milimetreye bir rakam düşecek şekilde yazıldığını varsayalım. Oluşacak kağıt şerit dünyanın ekvatordaki çevresine sarılsa kaç tam tur yapar? (Dünyanın ekvatordaki yarıçapını 6378,14 km alınız, π= 3.14)

"The Question of Prime Numbers connected to Number Theory Slides

SOURCE: BİLGEM dergisi 6.sayı-sayfa 170

http://www.uekae.tubitak.gov.tr/uekae_content_files/flash/UEKAE_dergi_sayfa_flash/sayi_6/Sayi6.pdf

cevap 15

(i) Üç sayı da asaldır.
(ii) Yaklaşık $1{,}275 \cdot 10^{27}$ tam tur.

Sanıda işaret edilen dizinin ilk terimlerini yazalım:

$p_1 = 2^2 - 1 = 3,\ \ p_2 = 2^3 - 1 = 7,\ \ p_3 = 2^7 - 1 = 127$

Bu sayıların üçü de asaldır. Sonraki terim

$p_4 = 2^{127} - 1$ de asaldır (ve bu ilk 4 terim, aynı zamanda Mersenne asalıdır). Sonraki terim

$p_5 = 2^{2^{127}-1} - 1 \approx 2^{2^{127}}$, çok büyük bir sayıdır. Bu sayının kaç basamaklı olduğunu kestirmek için 10 tabanına göre logaritmasını kullanalım:

$\log_{10}(p_5) = \log_{10}(2^{2^{127}}) = 2^{127} \cdot \log_{10} 2 \approx 5{,}1 \cdot 10^{37}$

olduğundan, sayı yaklaşık olarak $5{,}1 \cdot 10^{37}$ basamaklıdır. Dünyanın ekvatordaki çevresini

$2 \cdot \pi \cdot 6378{,}14$ km $\approx 4 \cdot 10^{10}$ mm olarak hesaplarsak, soruda işaret edilen kağıt şeridin dünyanın ekvatordaki çevresini, yaklaşık

$\dfrac{5{,}1 \cdot 10^{37}}{4 \cdot 10^{10}} = 1{,}275 \cdot 10^{27}$ kere sarabileceğini buluruz.

SOURCE: BİLGEM dergisi 7.sayı-sayfa 116

http://www.uekae.tubitak.gov.tr/uekae_content_files/flash/UEKAE_dergi_sayfa_flash/sayi_7/Sayi7.pdf

Relations on $\mathbb{Z}$:	$<$	$\leq$	$=$	$\mid$	$\nmid$	$\neq$
Reflexive	no	yes	yes	yes	no	no
Symmetric	no	no	yes	no	no	yes
Transitive	yes	yes	yes	yes	no	no

The Table Of Relations related to Relation Slides page7-10.

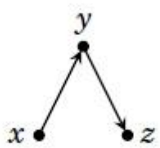
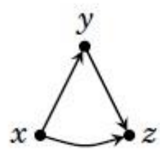
SOURCE: http://www.people.vcu.edu/~rhammack/BookOfProof/Relations.pdf

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

The Addition and Multiplication Tables for Z5 connected to Relation Slides page 30-36.

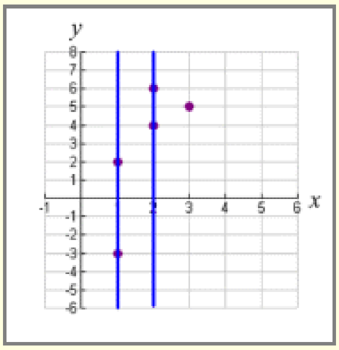
SOURCE: http://www.people.vcu.edu/~rhammack/BookOfProof/Relations.pdf

1.	A relation is **reflexive** if for each point x ...		...there is a loop at x:	
2.	A relation is **symmetric** if whenever there is an arrow from x to y ...		...there is also an arrow from y back to x:	
3.	A relation is **transitive** if whenever there are arrows from x to y and y to z ...		...there is also an arrow from x to z:	
	(If $x = z$, this means that if there are arrows from x to y and from y to x ...		...there is also a loop from x back to x.)	

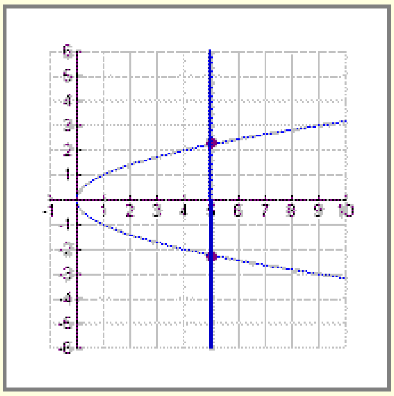
The Table Of Relations related to Relation Slides page7-10.

SOURCE: http://www.people.vcu.edu/~rhammack/BookOfProof/Relations.pdf

The following are examples of relations. Notice that a vertical line may intersect a relation in more than one location.

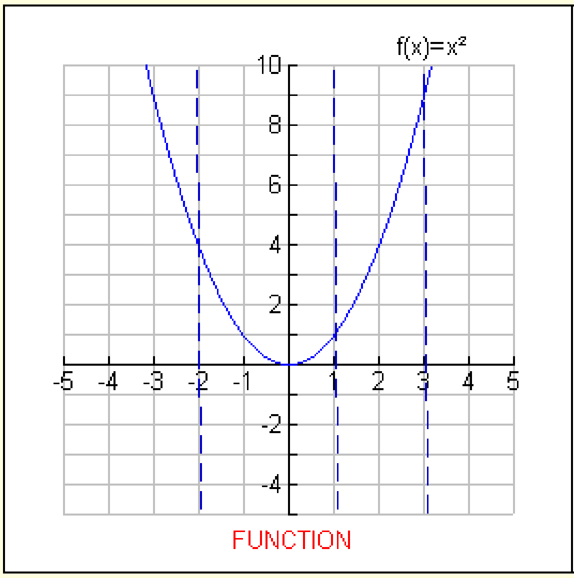


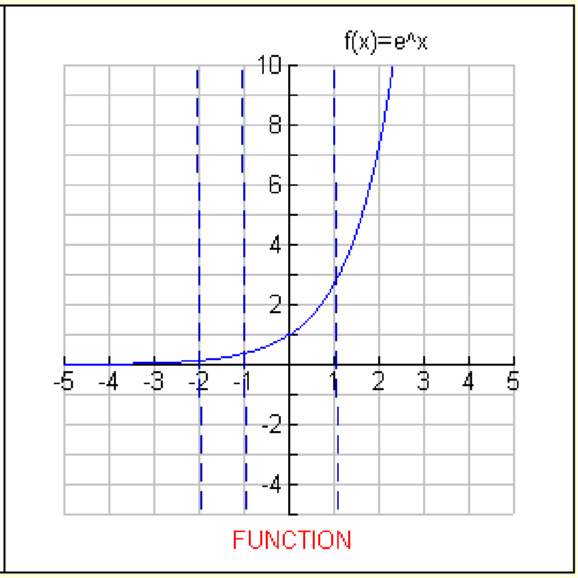
This set of 5 points is a relation.
{(1,2), (2, 4), (3, 5), (2, 6), (1, -3)}
Notice that vertical lines may intersect more than one point at a time.



This parabola is also a relation.
Notice that a vertical line can intersect this graph twice.

Vertical line test: each vertical line drawn through the graph will intersect a **function** in only one location.





The graphs of differences between relations and functions related to Sets and Relations Slides.

SOURCE: http://www.regentsprep.org/Regents/math/algtrig/ATP5/Lfunction.htm