Discrete Mathematics CS 2610

March 17, 2024

Number Theory

- Temel sayı teorisi, genellikle tam sayılar ve bu sayıların özellikleri veya rasyonel sayılarla ilgilenir.
- Özellikle tam sayılar arasındaki bölünebilirlik konularını ele alır. Uygulama Alanları: Kriptografi, E-ticaret, Ödeme Sistemleri, Rastgele Sayı Üretimi, Kodlama Teorisi, Hash Fonksiyonları.

- Some Applications
  - Cryptography
    - E-commerce
    - Payment systems
    - …
  - Random number generation
  - Coding theory
  - Hash functions (as opposed to stew functions ☺)

Number Theory - Division

Let a, b and c be integers, st $a \neq 0$, we say that "a divides b" or $a|b$ if there is an integer c where

$$b = a \cdot c \,.$$

- a and c are said to ***divide b*** (or are ***factors***)

$$a \mid b \wedge c \mid b$$

- b is a ***multiple*** of both a and c

Example:

$5 \mid 30$ and $5 \mid 55$ but $5 \nmid 27$

Number Theory - Division

Theorem 3.4.1: for all $a, b, c \in \mathbf{Z}$:

1. $a|0$
2. $(a|b \wedge a|c) \rightarrow a \mid (b + c)$
3. $a|b \rightarrow a|bc$ for all integers c
4. $(a|b \wedge b|c) \rightarrow a|c$

Proof: (2) $a|b$ means $b = ap$, and $a|c$ means $c = aq$

$b + c = ap + aq = a(p + q)$

therefore, $a|(b + c)$, or $(b + c) = ar$ where $r = p+q$

Proof: (4) $a|b$ means $b = ap$, and $b|c$ means $c = bq$

$c = bq = apq$

therefore, $a|c$ or $c = ar$ where $r = pq$

Division

Remember long division?

$$\begin{array}{r} 3 \\ 30\overline{)109} \\ \underline{90} \\ 19 \end{array}$$

$109 = 30 \cdot 3 + 19$

$a = dq + r$ (dividend = divisor · quotient + remainder)

The Division Algorithm

Division Algorithm Theorem: Let a be an integer, and d be a positive integer. There are unique integers q, r with $r \in \{0,1,2,\ldots,d-1\}$ (ie, $0 \le r < d$) satisfying

$$a = dq + r$$

- d is the divisor (bölen)
- q is the quotient (bölüm)

  q = a **div** d

- r is the remainder (kalan)

  r = a **mod** d

Mod Operation

Let $a, b \in \mathbf{Z}$ with $b > 1$.

$$a = q \cdot b + r, \text{ where } 0 \le r < b$$

Then a **mod** b denotes the remainder r from the division "algorithm" with dividend a and divisor b

109 **mod** 30 = ?

- $0 \le a \textbf{ mod } b \le b - 1$

Modular Arithmetic

- Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$

  Then *a is congruent (denk) to b modulo m* **iff** $m \mid (a - b)$.
- Notation:
  - "$a \equiv b \pmod{m}$" reads a is congruent to b modulo m
  - "$a \not\equiv b \pmod{m}$" reads a is not congruent to b modulo m.
- Examples:
  - $5 \equiv 25 \pmod{10}$
  - $5 \not\equiv 25 \pmod{3}$

Modular Arithmetic

Theorem 3.4.3: Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then

$$a \equiv b \pmod{m} \text{ iff } a \bmod m = b \bmod m$$

Proof: (1) given $a \bmod m = b \bmod m$ we have

$a = ms + r$ or $r = a - ms$,

$b = mp + r$ or $r = b - mp$,

$a - ms = b - mp$

which means $a - b = ms - mp$

$= m(s - p)$

so $m \mid (a - b)$ which means

$a \equiv b \pmod{m}$

Modular Arithmetic

Theorem 3.4.3: Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then
$a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

Proof: (2) given $a \equiv b \pmod{m}$ we have $m \mid (a - b)$

let $a = mq_a + r_a$ and $b = mq_b + r_b$

so, $m \mid ((mq_a + r_a) - (mq_b + r_b))$

or $m \mid m(q_a - q_b) + (r_a - r_b)$

recall $0 \le r_a < m$ and $0 \le r_b < m$

therefore $(r_a - r_b)$ must be 0

that is, the two remainders are the same

which is the same as saying

$a \bmod m = b \bmod m$

Modular Arithmetic

Theorem 3.4.4: Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then:
$a \equiv b \pmod{m}$ **iff** there exists a k $\in \mathbf{Z}$ st

$$a = b + km.$$

Proof: a = b + km means
a – b = km which means
m | (a – b) which is the same as saying
$a \equiv b \pmod{m}$
(to complete the proof, reverse the steps)

Examples:

$27 \equiv 12 \pmod{5}$	$27 = 12 + 5k$	$k = 3$
$105 \equiv -45 \pmod{10}$	$105 = -45 + 10k$	$k = 15$

Modular Arithmetic

Theorem 3.4.5: Let $a, b, c, d \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

1. $a + c \equiv b + d \pmod{m}$,
2. $a - c \equiv b - d \pmod{m}$,
3. $ac \equiv bd \pmod{m}$

Proof: $a = b + k_1 m$ and $c = d + k_2 m$

$$a + c = b + d + k_1 m + k_2 m$$

or $a + c = b + d + m(k_1 + k_2)$

which is

$$a + c \equiv b + d \pmod{m}$$

others are similar

Modular Arithmetic - examples

- Hash Functions: record access scheme for finding a record very quickly based on some key value in the record. That is, there is a mapping between the key value and the memory location for the record.

Ex. h(k) = k mod m (an onto (örten) function, why?)

k is the record's key value

m is the number of memory locations

Collisions occur since h is not one-to-one (birebir). What then? Typically, invoke a secondary hash function or some other scheme (sequential search).

f(a)=3 ve f(b)=3 ise hash funct. Linked list ile bağlıyorsun genellikle

Modular Arithmetic - examples

Pseudorandom numbers: generated using the linear congruential method (doğrusal eşlik metodu)

m – modulus

a - multiplier

c – increment

x_0 – seed

$$2 \leq a < m, \quad 0 \leq c < m, \quad 0 \leq x_0 < m$$

Generate the set of PRNs $\{x_n\}$,asal sayı, with $0 \leq x_n < m$ for all n

$$X_{n+1} = (aX_n + c) \bmod m$$

(divide by m to get PRNs between 0 and 1)

Pseudonumber

1. Bir **başlangıç değeri (seed)** seçiyoruz:

   X_0

2. Formülü çalıştırıyoruz:

   $X_1 = (a \cdot X_0 + c) \bmod m$

   $X_2 = (a \cdot X_1 + c) \bmod m$

   $X_3 = (a \cdot X_2 + c) \bmod m$

   ...

3. Her X_n bir psödo-random sayıdır.

4. Eğer `0-1` arasında istiyorsak:

   $\mathbf{rn = X_n / m}$

$m = 9$, $a = 2$, $c = 5$, başlangıç $X_0 = 1$ olsun:

$X_1 = (2 \cdot 1 + 5) \bmod 9 = 7$

$X_2 = (2 \cdot 7 + 5) \bmod 9 = 1$ ← döngüye girdi

$\mathbf{X_{n+1} = (a \cdot X_n + c) \bmod m}$

Bu, bir sonraki "rastgele" sayıyı üretmek için kullanılan deterministik bir kuraldır.

- $\mathbf{X_n}$ → mevcut sayı
- $\mathbf{X_{n+1}}$ → bir sonraki sayı
- **a** → çarpan (multiplier)
- **c** → ek sabit (increment)
- **m** → modül (genelde büyük bir sayı veya asal sayı)

Modular Arithmetic - examples

cryptology: secret codes, encryption/decryption

Caesar encryption (positional 3-offset scheme)

For our 26 letters, assign integers 0-25

$f(p) = (p + 3) \bmod 26$

"PARK" maps to integers 15, 0, 17, 10 which are then encrypted into 18, 3, 20, 13 or "SDUN"

use the inverse $(p - 3) \bmod 26$ to decrypt back to "PARK"

Number Theory – Primes (Asal)

A positive integer $n > 1$ is called ***prime*** if it is only divisible by 1 and itself (i.e., only has 1 and itself as its positive factors).

Example: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 97

A number $n \geq 2$ which isn't prime is called ***composite***. (Iff there exists an a such that $a|n$ and $1 < a < n$)

Example:

All even numbers > 2 are composite.

By convention, 1 is neither prime or composite (birleşik sayı).

Number Theory - Primes

Fundamental Theorem of Arithmetic

Tüm birleşik sayıları asal sayıların artan sıralı çarpımı cinsinden gösterebiliriz

Examples:

- $2 = 2$
- $4 = 2 \cdot 2$
- $100 = 2 \cdot 2 \cdot 5 \cdot 5$
- $200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37$

Number Theory – Primality Testing

- How do you check whether a positive integer n is prime?

  - Solution:

    Start testing to see if prime p divides n ($2|n$, $3|n$, $5|n$, etc). When one is found, use the dividend and begin again. Repeat.

    Find prime factorization for 7007.
    2, 3, 5 don't divide 7007 but 7 does (1001)
    Now, 7 also divides 1001 (143)
    7 doesn't divide 143 but 11 does (13) and we're done.

Number Theory - Primes

Theorem 3.5.2 : If n is composite, then it has a prime factor (divisor) that is less than or equal to $\sqrt{n}$

Proof: if n is composite, we know it has a factor a with $1 < a < n$. IOW $n = ab$ for some $b > 1$. So, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ (note, if $a > \sqrt{n}$ and $b > \sqrt{n}$ then $ab > n$, nope). OK, both a and b are divisors of n, and n has a positive divisor not exceeding $\sqrt{n}$. Bu bölen ya asaldır ya da kendisinden küçük bir asal böleni vardır. Her iki durumda da n'nin $\leq \sqrt{n}$ asal böleni vardır.

*** Bir tamsayı, kareköküne eşit veya daha küçük herhangi bir asal sayıya bölünemiyorsa asaldır.

Number Theory – Prime Numbers

- **Theorem 3.5.4**: The number of primes not exceeding *n* is **asymptotic** to *n*/log *n* .

- i.e. $\lim_{n \to \infty} \Pi(n)/(n \log n) \to 1$, doğal logaritma
- 1000/math.log(1000). Pi(n) gerçekte ilgili sayıya kadar olan asal sayı adedi

$\Pi(n)$: number of prime numbers less than or equal to n

n	$\Pi(n)$	n/log n
1000	168	145
10000	1229	1086
100000	9592	8686
1000000	78498	72382
10000000	664579	620420
100000000	5761455	5428681

Number Theory – Prime Numbers

There are still plenty of things we don't know about primes:

* no cool function gives us primes, not even

  $f(n) = n^2 - n + 41$

* Goldbach's conjecture (varsayım) : every even integer n where n > 2 is the sum of two primes (18=13+5 ; 24= 19+5; 32=29+3)

* twin prime conjecture: there are infinitely many twin primes (ikiz asal) (pairs p and p+2, both prime 5 ve 7 gibi)

Greatest Common Divisor (ortak bölenlerin en büyüğü, obeb)

Let a, b be integers, $a \neq 0$, $b \neq 0$, not both zero.

The ***greatest common divisor*** of a and b is the biggest number d which divides both a and b.

Example: gcd(42,72)

Positive divisors of 42: 1,2,3,6,7,14,21

Positive divisors of 72: 1,2,3,4,6,8,9,12,24,36

gcd(42,72)=6

Finding the GCD

- If the prime factorizations are written as

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \quad \text{and} \quad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$$

then the GCD is given by:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,b_n)}.$$

Example:

- $a = 42 = 2 \cdot 3 \cdot 7 \qquad = 2^1 \cdot 3^1 \cdot 7^1$
- $b = 72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \qquad = 2^3 \cdot 3^2 \cdot 7^0$
- $\gcd(42, 72) \qquad = 2^1 \cdot 3^1 \cdot 7^0 = 2 \cdot 3 = 6$

Least Common Multiple (ortak katların en küçüğü, okek)

- a ve b tarafından ortak bölünebilen en küçük sayıya ortak katların en küçüğü denir

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}.$$

Example: $\operatorname{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^4 3^5 7^2$

Least Common Multiple

Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$$

Modular Exponentiation

- Let b be base, n, m large integers, $b < m$.
- «b» taban, «n» ve «m» büyük sayılar olsun, b<m
- The modular exponentiation is computed as

$$b^n \bmod m$$

Fundamental in cryptography: RSA encryption

How can we compute the modular exponentiation ?

Modular Exponentiation

For large b, n and m, we can compute the modular exponentiation using the following property:

$a \cdot b \bmod m = (a \bmod m)\,(b \bmod m) \bmod m$

(Mod5)91= 13*7 = 3*2 (mod 5)=1

Therefore, $b^n \pmod{m} = (b \bmod m)^n \pmod{m}$

In fact, we can take (mod m) after each multiplication to keep all values low.

Example

- Find $37^5 \pmod 5$

$37^5 \pmod 5 = (37 \pmod 5)^5 \pmod 5 = 2^5 \pmod 5$

$2^5 \pmod 5 = 2*2*2*2*2 \pmod 5 = 4*2*2*2 \pmod 5 =$
$8*2*2 \pmod 5 = 3*2*2 \pmod 5 = 6*2 \pmod 5 =$
$1*2 \pmod 5 = 2 \pmod 5 = 2$

Can you see a way to shorten this process?

Use results you have already calculated

$2^5 \pmod 5 = 4*4*2 \pmod 5 = 16*2 \pmod 5 = 2$

For large exponents this can make a big difference!

örnekler

- 3^2000 mod 20 =? 1?
- 33^125 mod 7=?

Fermat'nın Küçük Teoremi'ni uygulayalım: Fermat'nın Küçük Teoremi'ne göre, asal bir p sayısı ve a sayısı p'ye tam bölünmüyorsa:

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

Burada $p = 7$, $a = 5$, yani:

$$5^6 \equiv 1 \pmod{7}$$

Cryptography

- Cryptology is the study of secret (coded) messages.
  - *Cryptography* – Methods for encrypting (şifreleme) and decrypting (şifre çözme) secret messages using secret keys.
    - Encryption,şifreleme, is the process of transforming a message to an unreadable form.
    - Decryption, çözümleme, is the process of transforming an encrypted message back to its original form.
    - Both encryption and decryption require the use of some secret knowledge known as the secret key.
  - *Cryptoanalysis* – Methods for decrypting an encrypted message without knowing the secret keys.

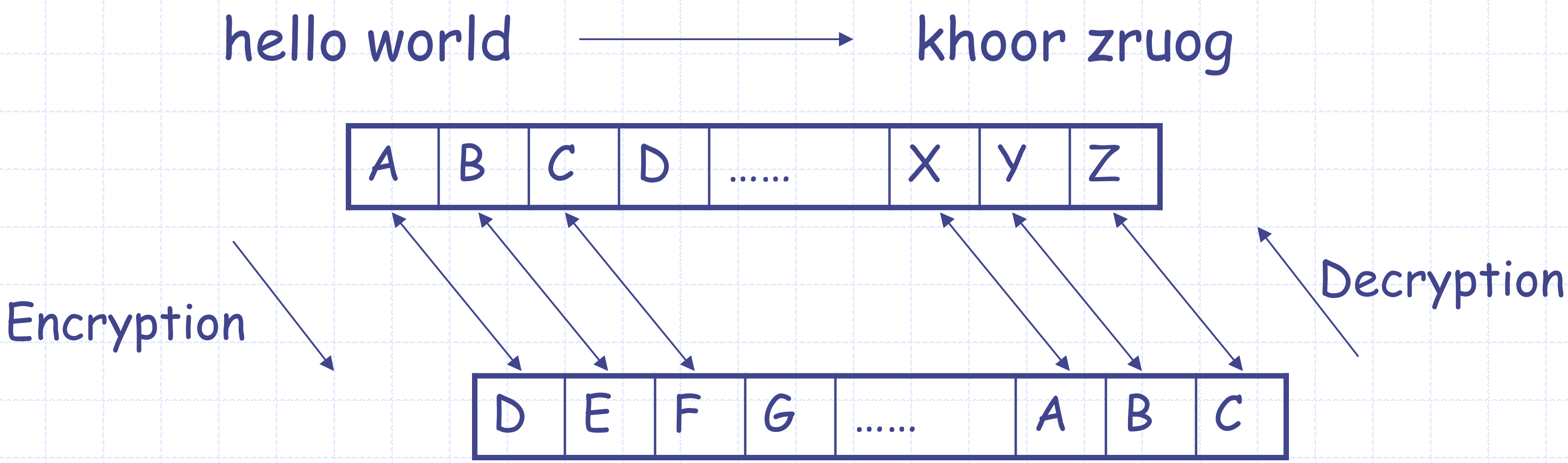
Cryptography - Caesar's shift cypher

Encryption

- Shift each letter in the message three letters forward in the alphabet.

Decryption

- Shift each letter in the message three letters backward in the alphabet.



Public Key Cryptography

- ***Public key cryptosystems use two keys***
  - **Public key** to encrypt the message
    - Known to everybody
  - **Private Key** to decrypt the encrypted message (şifreyi çözmek için kullanılan ve sadece yetkili kişide olan gizli anahtar)
    - It is kept secret.
    - It is computationally infeasible to guess the Private Key
- RSA one of the most widely used ***Public key cryptosystem***

Ronald Rivest, Adi Shamir, and Leonard Adleman

RSA Basis

- Let p and q be two large primes, and $e \in Z$ such that
  $$gcd(e,(p-1)(q-1)) = 1$$
  and d (the decryption key) is an integer such that
  $$de \equiv 1 \pmod{(p-1)(q-1)}$$
- p and q are large primes,over 100 digits each.
- Public Key
  - $n=pq$ (the modulus)
  - e (the public exponent)
  - It is common to choose a small public exponent for the public key.
- Private Key
  - d (the private exponent)

RSA

- Encryption
  - Let M be a message such that $M < n$
  - Compute $C = M^e \bmod n$
    - This can be done using *Binary Modular Exponentiation*
- Decryption
  - Compute $M = C^d \pmod{pq}$

Why Does RSA Work?

- RSA yönteminin doğruluğu, ne p ne de q'nun M'yi bölmediği varsayımından (ki bu çoğu mesaj için doğru olacaktır) ve aşağıdaki iki teoremden kaynaklanmaktadır.
- 1.Fermat's Little Theorem

  If p is a prime and a is an integer not divisible by p-1 then $a^{p-1} \equiv 1 \pmod{p}$.

  P=7, a= 9, 9^6 (mod 7)= 2^6 (mod7)=1
- 2. The Chinese Remainder Theorem

  Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers. The system (aralarında asal)

  $x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$ … $x \equiv a_n \pmod{m_n}$

  has a unique solution modulo $m_1 m_2 \ldots m_n$ – i.e., there is only one x such that $0 \leq x < m_1 m_2 \ldots m_n$ that satisfies the above congruencies.(yukardaki eşitlikleri)

Çinli Kalan Teoremi

Çinlilerin kalan teoremi

Çinlilerin kalan teoremi, "3'e bölündüğünde 2, 5'e bölündüğünde 3, 7'ye bölündüğünde 4 kalanını veren sayıyı bulun" tipinden problemleri çözmek için kullanılan teorem. buna göre: 3'e bölündüğünde 2 kalanını veren sayılar 3.k+2 şeklindedir. (2, 5, 8, ...) 5'e bölündüğünde 3 kalanını veren sayılar 5.l+3 şeklindedir. (3, 8, 13, ...) bu durumda sayımız 15m+8 şeklindedir. (8, 23, 38, 53, ...) 7'ye bölündüğünde 4 kalanını veren sayılar 7.n+4 şeklindedir. (4, 11, 18, ..., 46, 53, ...) bu durumda da sayımız 105.p+53 şeklindedir.

$n_1, n_2, \ldots, n_k$ pozitif, çiftli aralarında asal Tamsayı olsun. Bu durumda, Verilen herhangi $a_1, a_2, \ldots, a_k$, tamsayıları için bir x tamsayısı vardır ki sistemin eşzamanlı uygun bir çözümüdür.

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Bundan başka, Tüm Çözümler x Bu sistem uyumlu olan modulo $N = n_1 n_2 \ldots n_k$.

Böylece $x \equiv y \pmod{n_i}$ tüm $1 \leq i \leq k$, ancak ve ancak $x \equiv y \pmod{N}$.

Sometimes, the simultaneous congruences can be solved even if the n_i's are not pairwise coprime. A solution x exists if and only if:

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)} \qquad \text{for all } i \text{ and } j.$$

All solutions x are then congruent modulo the least common multiple of the n_i.

Versions of the Chinese remainder theorem were also known to Brahmagupta (7th century), and appear in Fibonacci's Liber Abaci (1202).

Çinli Kalan Teoremi

İspat. $n = n_1 n_2 \cdots n_k$ olsun.
$1 \leq i \leq k$ için $\left(\frac{n}{n_i}, n_i\right) = 1$ olduğundan $\frac{n}{n_i} s_i \equiv r_i \mod n_i$ denklik sistemini sağlayan s_i vardır.
$x \equiv \sum_{i=1}^{k} \frac{n}{n_i} s_i$ olsun.

Aşağıdaki denklik sistemini çözünüz.

$$\begin{aligned} x &\equiv 2 \mod 7 \\ x &\equiv 4 \mod 9 \\ x &\equiv 1 \mod 10. \end{aligned}$$

Çözüm. $n = 7 \cdot 9 \cdot 10 = 630$, $\frac{n}{n_1} = 90$, $\frac{n}{n_2} = 70$ ve $\frac{n}{n_3} = 63$ olduğundan

$$\begin{aligned} 90s_1 \equiv 2 \mod 7 &\Rightarrow 6s_1 \equiv 2 \mod 7 \Rightarrow s_1 \equiv 6^{-1} \cdot 2 \equiv 6 \cdot 2 \equiv 5 \mod 7 \\ 70s_2 \equiv 4 \mod 9 &\Rightarrow 7s_2 \equiv 4 \mod 9 \Rightarrow s_2 \equiv 7^{-1} \cdot 4 \equiv 4 \cdot 4 \equiv 7 \mod 9 \\ 63s_3 \equiv 1 \mod 10 &\Rightarrow 3s_3 \equiv 1 \mod 10 \Rightarrow s_3 \equiv 3^{-1} \cdot 1 \equiv 7 \mod 10 \end{aligned}$$

bulunur. Buradan $x \equiv \sum_{i=1}^{3} \frac{n}{n_i} s_i = 90 \cdot 5 + 70 \cdot 7 + 63 \cdot 7 = 1381$ olur. Çözüm mod 630 da tek olduğundan $x = 1381 \equiv 121 \mod 630$ elde edilir.

Why Does RSA Work?

- Since $de \equiv 1 \pmod{(p-1)(q-1)}$, we can conclude that $de=1+k(p-1)(q-1)$.
- Therefore $C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}$.
- Assuming $\gcd(M,p) = \gcd(M,q) = 1$, we can conclude (by Fermat's Little Theorem) that. M, p-1'e tam bölünmüyor (1 kalıyor)
  - $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M \pmod{p}$
  - $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M \pmod{q}$
- By the Chinese Remainder Theorem, we can conclude that
  - $C^d \equiv M \pmod{pq}$
    - Recall that $n = pq$

RSA Example

- Let $p = 61$ and $q = 53$
  - Then $n = pq = 3233$
- Let $e = 17$ and $d = 2753$
  - $de \equiv 1 \pmod{(p-1)(q-1)}$
  - Note $17 * 2753 = 46801 = 1+ 15*60*52$
- Public keys: e, n
- Private key: d
- Encrypt 123
  - $123^{17} \pmod{3233} = 855$
- Decrypt 855
  - $855^{2753} \pmod{3233} = 123$, tek bir d var bunu sağlayan
- We need clever exponentiation techniques!

Breaking RSA

How to break the system

1. An attacker discovers the numbers *p* and *q*
   - Find the prime factorization of *n*
   - Computationally difficult when *p* and *q* are chosen properly.
   - The modulus *n* must be at least 2048 bits long
     - On May 10, 2005, RSA-200, a 200-digit number module was factored into two 100-digit primes by researchers in Germany
       - The effort started during Christmas 2003 using several computers in parallel.
       - Equivalent of 55 years on a single 2.2 GHz Opteron CPU

RSA – In practice

- How to break the system

2. Find *e*-th roots mod n.
   - *The encrypted message* C *is obtained as*
     - $C = M^e \bmod n$
   - No general methods are currently known to find the e-th roots mod n, except for special cases.

Review of Secret Key (Symmetric) Cryptography

- Confidentiality (gizlilik)
  - stream ciphers (uses PRNG)
  - block ciphers with encryption modes
- Integrity (bütünlük)
  - Cryptographic hash functions
  - Message authentication code (keyed hash functions)
- Limitation: sender and receiver must share the same key
  - Needs secure channel for key distribution
  - Impossible for two parties having no prior relationship
  - Needs many keys for n parties to communicate

RSA Algorithm

- Invented in **1978** by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman
  - Published as R L Rivest, A Shamir, L Adleman, "*On Digital Signatures and Public Key Cryptosystems*", Communications of the ACM, vol 21 no 2, pp120-126, Feb 1978
- Security relies on the difficulty of factoring large composite numbers
- Essentially the same algorithm was discovered in 1973 by Clifford Cocks, who works for the British intelligence

RSA Public Key Crypto System

Key generation:

1. Select 2 large prime numbers of about the same size, p and q

    Typically each p, q has between 512 and 2048 bits

2. Compute $n = pq$, and $\Phi(n) = (q-1)(p-1)$
3. Select e, $1 < e < \Phi(n)$, s.t. $\gcd(e, \Phi(n)) = 1$

    Typically e=3 or e=65537

4. Compute d, $1 < d < \Phi(n)$ s.t. $ed \equiv 1 \bmod \Phi(n)$

    Knowing $\Phi(n)$, d easy to compute.

Public key: (e, n)
Private key: d

RSA Description (cont.)

Encryption

Given a message M, $0 < M < n$ $\quad M \in Z_n - \{0\}$

use public key (e, n)

compute $C = M^e \bmod n$ $\quad C \in Z_n - \{0\}$

Decryption

Given a ciphertext C, use private key (d)

Compute $C^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n = M$

RSA Example

- $p = 11, q = 7, n = 77, \Phi(n) = 60$,((q-1)(p-1))
- $d = 13, e = 37$ (ed = 481; ed mod 60 = 1)
  - $de \equiv 1 \pmod{(p-1)(q-1)}$
- Let $M = 15$. Then $C \equiv M^e \bmod n$
  - $C \equiv 15^{37} \pmod{77} = 71$
- $M \equiv C^d \bmod n$
  - $M \equiv 71^{13} \pmod{77} = 15$