Bahan Kuliah ke-3

IF5054 Kriptografi

Teori Bilangan (*Number Theory*)

Disusun oleh:

Ir. Rinaldi Munir, M.T.

Departemen Teknik Informatika
Institut Teknologi Bandung
2004

3. Teori Bilangan

- Teori bilangan (*number theory*) adalah teori yang mendasar dalam memahami algoritma kriptografi

- Bilangan yang dimaksudkan adalah bilangan bulat (*integer*)

3.1 Bilangan Bulat

- Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal, misalnya 8, 21, 8765, -34, 0

- Berlawanan dengan bilangan bulat adalah bilangan riil yang mempunyai titik desimal, seperti 8.0, 34.25, 0.02.

Sifat Pembagian pada Bilangan Bulat

- Misalkan a dan b adalah dua buah bilangan bulat dengan syarat $a \neq 0$. Kita menyatakan bahwa a **habis membagi** b (*a divides b*) jika terdapat bilangan bulat c sedemikian sehingga $b = ac$.

- Notasi: $a \mid b$ jika $b = ac$, $c \in \mathbf{Z}$ dan $a \neq 0$. ($\mathbf{Z}$ = himpunan bilangan bulat)

- Kadang-kadang pernyataan "*a* habis membagi *b*" ditulis juga "*b* **kelipatan** *a*".

- **Contoh 1**: $4 \mid 12$ karena $12 \div 4 = 3$ (bilangan bulat) atau $12 = 4 \times 3$. Tetapi $4 \mid 13$ karena $13 \div 4 = 3.25$ (bukan bilangan bulat).

Teorema 1 (Teorema Euclidean). Misalkan m dan n adalah dua buah bilangan bulat dengan syarat $n > 0$. Jika m dibagi dengan n maka terdapat dua buah bilangan bulat unik q (*quotient*) dan r (*remainder*), sedemikian sehingga

$$m = nq + r \qquad (1)$$

dengan $0 \le r < n$.

Contoh 2.
(i) 1987 dibagi dengan 97 memberikan hasil bagi 20 dan sisa 47:

$$1987 = 97 \cdot 20 + 47$$

(ii) –22 dibagi dengan 3 memberikan hasil bagi –8 dan sisa 2:

$$-22 = 3(-8) + 2$$

tetapi $-22 = 3(-7) - 1$ salah karena $r = -1$ tidak memenuhi syarat $0 \le r < n$.

3.2 Pembagi Bersama Terbesar (PBB)

- Misalkan a dan b adalah dua buah bilangan bulat tidak nol. Pembagi bersama terbesar (PBB – **greatest common divisor** atau *gcd*) dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga $d \mid a$ dan $d \mid b$. Dalam hal ini kita nyatakan bahwa PBB(a, b) = d.

- **Contoh 3.** Faktor pembagi 45: 1, 3, 5, 9, 15, 45;
  Faktor pembagi 36: 1, 2, 3, 4, 9, 12, 18, 36;
  Faktor pembagi bersama dari 45 dan 36 adalah 1, 3, 9
  PBB(45, 36) = 9.

Algoritma Euclidean

- Algoritma Euclidean adalah algoritma untuk mencari PBB dari dua buah bilangan bulat.
- Euclid, penemu algoritma Euclidean, adalah seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam bukunya yang terkenal, *Element*.
- Diberikan dua buah bilangan bulat tak-negatif m dan n ($m \geq n$). Algoritma Euclidean berikut mencari pembagi bersama terbesar dari m dan n.

Algoritma Euclidean

1. Jika $n = 0$ maka
   m adalah PBB(m, n);
   stop.
   tetapi jika $n \neq 0$,
   lanjutkan ke langkah 2.
2. Bagilah m dengan n dan misalkan r adalah sisanya.
3. Ganti nilai m dengan nilai n dan nilai n dengan nilai r, lalu ulang kembali ke langkah 1.

Contoh 4. $m = 80$, $n = 12$ dan dipenuhi syarat $m \geq n$

$$80 = 6 \cdot 12 + 8$$
$$12 = 1 \cdot 8 + 4$$
$$8 = 2 \cdot 4 + 0$$

Sisa pembagian terakhir sebelum 0 adalah 4, maka PBB(80, 12) = 4.

3.3 Relatif Prima

- Dua buah bilangan bulat *a* dan *b* dikatakan *relatif prima* jika PBB(*a*, *b*) = 1.
- **Contoh 5.** 20 dan 3 relatif prima sebab PBB(20, 3) = 1. Begitu juga 7 dan 11 relatif prima karena PBB(7, 11) = 1. Tetapi 20 dan 5 tidak relatif prima sebab PBB(20, 5) = 5 ≠ 1.
- Jika *a* dan *b* relatif prima, maka terdapat bilangan bulat *m* dan *n* sedemikian sehingga

$$ma + nb = 1 \qquad (2)$$

- **Contoh 6.** Bilangan 20 dan 3 adalah relatif prima karena PBB(20, 3) =1, atau dapat ditulis

$$2 \cdot 20 + (-13) \cdot 3 = 1$$

dengan $m = 2$ dan $n = -13$. Tetapi 20 dan 5 tidak relatif prima karena PBB(20, 5) = 5 ≠ 1 sehingga 20 dan 5 tidak dapat dinyatakan dalam $m \cdot 20 + n \cdot 5 = 1$.

3.4 Aritmetika Modulo

- Misalkan *a* adalah bilangan bulat dan *m* adalah bilangan bulat > 0. Operasi *a* mod *m* (dibaca "*a* modulo *m*") memberikan sisa jika *a* dibagi dengan *m.*
- Notasi: *a* mod *m* = *r* sedemikian sehingga $a = mq + r$, dengan $0 \le r < m$.

- Bilangan *m* disebut **modulus** atau **modulo**, dan hasil aritmetika modulo *m* terletak di dalam himpunan {0, 1, 2, …, *m* – 1} (mengapa?).

Contoh 7. Beberapa hasil operasi dengan operator modulo:

(i) 23 mod 5 = 3 (23 = 5 · 4 + 3)
(ii) 27 mod 3 = 0 (27 = 3 · 9 + 0)
(iii) 6 mod 8 = 6 (6 = 8 · 0 + 6)
(iv) 0 mod 12 = 0 (0 = 12 · 0 + 0)
(v) – 41 mod 9 = 4 (–41 = 9 (–5) + 4)
(vi) – 39 mod 13 = 0 (–39 = 13(–3) + 0)

Penjelasan (v): Karena *a* negatif, bagi |*a*| dengan *m* mendapatkan sisa *r*'. Maka *a* mod *m* = *m* – *r*' bila *r*' ≠ 0. Jadi |– 41| mod 9 = 5, sehingga –41 mod 9 = 9 – 5 = 4.

Kongruen

- Misalnya 38 mod 5 = 3 dan 13 mod 5 = 3, maka kita katakan 38 ≡ 13 (mod 5) (baca: 38 kongruen dengan 13 dalam modulo 5).

- Misalkan *a* dan *b* adalah bilangan bulat dan *m* adalah bilangan > 0, maka $a \equiv b \pmod{m}$ jika *m* habis membagi *a* – *b*.

- Jika *a* tidak kongruen dengan *b* dalam modulus *m*, maka ditulis $a \not\equiv b \pmod{m}$.

Contoh 8.

17 ≡ 2 (mod 3) (3 habis membagi 17 – 2 = 15)
–7 ≡ 15 (mod 11) (11 habis membagi –7 – 15 = –22)
12 ≡/ 2 (mod 7) (7 tidak habis membagi 12 – 2 = 10)
–7 ≡/ 15 (mod 3) (3 tidak habis membagi –7 – 15 = –22)

- Kekongruenan $a \equiv b \pmod{m}$ dapat pula dituliskan dalam hubungan

$$a = b + km \qquad (3)$$

yang dalam hal ini k adalah bilangan bulat.

Contoh 9.

$17 \equiv 2 \pmod 3$ dapat ditulis sebagai $17 = 2 + 5 \cdot 3$
$-7 \equiv 15 \pmod{11}$ dapat ditulis sebagai $-7 = 15 + (-2)11$

- Berdasarkan definisi aritmetika modulo, kita dapat menuliskan $a \bmod m = r$ sebagai

$$a \equiv r \pmod m$$

Contoh 10.

Beberapa hasil operasi dengan operator modulo berikut:

(i) $23 \bmod 5 = 3$ dapat ditulis sebagai $23 \equiv 3 \pmod 5$
(ii) $27 \bmod 3 = 0$ dapat ditulis sebagai $27 \equiv 0 \pmod 3$
(iii) $6 \bmod 8 = 6$ dapat ditulis sebagai $6 \equiv 6 \pmod 8$
(iv) $0 \bmod 12 = 0$ dapat ditulis sebagai $0 \equiv 0 \pmod{12}$
(v) $-41 \bmod 9 = 4$ dapat ditulis sebagai $-41 \equiv 4 \pmod 9$
(vi) $-39 \bmod 13 = 0$ dapat ditulis sebagai $-39 \equiv 0 \pmod{13}$

Teorema 2. Misalkan m adalah bilangan bulat positif.

1. Jika $a \equiv b \pmod m$ dan c adalah sembarang bilangan bulat maka
   (i) $(a + c) \equiv (b + c) \pmod m$
   (ii) $ac \equiv bc \pmod m$
   (iii) $a^p \equiv b^p \pmod m$ untuk suatu bilangan bulat tak negatif p.

2. Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$, maka
   (i) $(a + c) \equiv (b + d) \pmod m$
   (ii) $ac \equiv bd \pmod m$

Bukti (hanya untuk 1(ii) dan 2(i) saja):

1(ii) $a \equiv b \pmod m$ berarti:

$\Leftrightarrow a = b + km$
$\Leftrightarrow a - b = km$
$\Leftrightarrow (a - b)c = ckm$
$\Leftrightarrow ac = bc + Km$
$\Leftrightarrow ac \equiv bc \pmod m$ ■

2(i) $a \equiv b \pmod m \Leftrightarrow a = b + k_1 m$
$c \equiv d \pmod m \Leftrightarrow c = d + k_2 m +$
$\Leftrightarrow (a + c) = (b + d) + (k_1 + k_2)m$
$\Leftrightarrow (a + c) = (b + d) + km \quad (k = k_1 + k_2)$
$\Leftrightarrow (a + c) = (b + d) \pmod m$ ■

Contoh 11.

Misalkan $17 \equiv 2 \pmod 3$ dan $10 \equiv 4 \pmod 3$, maka menurut Teorema 2,

$17 + 5 = 2 + 5 \pmod 3 \Leftrightarrow 22 = 7 \pmod 3$
$17 \cdot 5 = 5 \cdot 2 \pmod 3 \Leftrightarrow 85 = 10 \pmod 3$
$17 + 10 = 2 + 4 \pmod 3 \Leftrightarrow 27 = 6 \pmod 3$
$17 \cdot 10 = 2 \cdot 4 \pmod 3 \Leftrightarrow 170 = 8 \pmod 3$

- Perhatikanlah bahwa Teorema 2 tidak memasukkan operasi pembagian pada aritmetika modulo karena jika kedua ruas dibagi dengan bilangan bulat, maka kekongruenan tidak selalu dipenuhi. Misalnya:
  (i) $10 \equiv 4 \pmod 3$ dapat dibagi dengan 2 karena $10/2 = 5$ dan $4/2 = 2$, dan $5 \equiv 2 \pmod 3$
  (ii) $14 \equiv 8 \pmod 6$ tidak dapat dibagi dengan 2, karena $14/2 = 7$ dan $8/2 = 4$, tetapi $7 \not\equiv 4 \pmod 6$.

Balikan Modulo (modulo invers)

- Jika a dan m relatif prima dan $m > 1$, maka kita dapat menemukan balikan (*invers*) dari a modulo m. Balikan dari a modulo m adalah bilangan bulat $\bar{a}$ sedemikian sehingga

  $$a\bar{a} \equiv 1 \pmod m$$

  Bukti: Dari definisi relatif prima diketahui bahwa PBB(a, m) = 1, dan menurut persamaan (2) terdapat bilangan bulat p dan q sedemikian sehingga

  $$pa + qm = 1$$

  yang mengimplikasikan bahwa

  $$pa + qm \equiv 1 \pmod m$$

  Karena $qm \equiv 0 \pmod m$, maka

  $$pa \equiv 1 \pmod m$$

  Kekongruenan yang terakhir ini berarti bahwa p adalah balikan dari a modulo m. ■

- Pembuktian di atas juga menceritakan bahwa untuk mencari balikan dari *a* modulo *m*, kita harus membuat kombinasi lanjar dari *a* dan *m* sama dengan 1. Koefisien *a* dari kombinasi lanjar tersebut merupakan balikan dari *a* modulo *m.*

Contoh 12.
Tentukan balikan dari 4 (mod 9), 17 (mod 7), dan 18 (mod 10).

Penyelesaian:

(a) Karena PBB(4, 9) = 1, maka balikan dari 4 (mod 9) ada. Dari algoritma Euclidean diperoleh bahwa

$$9 = 2 \cdot 4 + 1$$

Susun persamaan di atas menjadi

$$-2 \cdot 4 + 1 \cdot 9 = 1$$

Dari persamaan terakhir ini kita peroleh –2 adalah balikan dari 4 modulo 9. Periksalah bahwa

$-2 \cdot 4 \equiv 1 \pmod 9$ (9 habis membagi $-2 \cdot 4 - 1 = -9$)

(b) Karena PBB(17, 7) = 1, maka balikan dari 17 (mod 7) ada. Dari algoritma Euclidean diperoleh rangkaian pembagian berikut:

$17 = 2 \cdot 7 + 3$ (i)
$7 = 2 \cdot 3 + 1$ (ii)
$3 = 3 \cdot 1 + 0$ (iii) (yang berarti: PBB(17, 7) = 1))

Susun (ii) menjadi:

$1 = 7 - 2 \cdot 3$ (iv)

Susun (i) menjadi

$3 = 17 - 2 \cdot 7$ (v)

Sulihkan (v) ke dalam (iv):

$1 = 7 - 2 \cdot (17 - 2 \cdot 7) = 1 \cdot 7 - 2 \cdot 17 + 4 \cdot 7 = 5 \cdot 7 - 2 \cdot 17$

atau

$-2 \cdot 17 + 5 \cdot 7 = 1$

Dari persamaan terakhir ini kita peroleh –2 adalah balikan dari 17 modulo 7.

$-2 \cdot 17 \equiv 1 \pmod 7$ (7 habis membagi $-2 \cdot 17 - 1 = -35$)

(c) Karena PBB(18, 10) = $2 \neq 1$, maka balikan dari 18 (mod 10) tidak ada.

Kekongruenan Lanjar

- Kekongruenan lanjar adalah kongruen yang berbentuk

  $ax \equiv b \pmod m$

  dengan m adalah bilangan bulat positif, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat.

- Nilai-nilai *x* dicari sebagai berikut:

  $ax = b + km$

  yang dapat disusun menjadi

  $$x = \frac{b + km}{a}$$

  dengan *k* adalah sembarang bilangan bulat. Cobakan untuk *k* = 0, 1, 2, … dan *k* = –1, –2, … yang menghasilkan *x* sebagai bilangan bulat.

Contoh 13.
Tentukan solusi: $4x \equiv 3 \pmod 9$ dan $2x \equiv 3 \pmod 4$

Penyelesaian:
(i) $4x \equiv 3 \pmod 9$

$$x = \frac{3 + k \cdot 9}{4}$$

$k = 0 \rightarrow x = (3 + 0 \cdot 9)/4 = 3/4$ (bukan solusi)
$k = 1 \rightarrow x = (3 + 1 \cdot 9)/4 = 3$
$k = 2 \rightarrow x = (3 + 2 \cdot 9)/4 = 21/4$ (bukan solusi)
$k = 3$, $k = 4$ tidak menghasilkan solusi
$k = 5 \rightarrow x = (3 + 5 \cdot 9)/4 = 12$
…
$k = –1 \rightarrow x = (3 – 1 \cdot 9)/4 = –6/4$ (bukan solusi)
$k = –2 \rightarrow x = (3 – 2 \cdot 9)/4 = –15/4$ (bukan solusi)
$k = –3 \rightarrow x = (3 – 3 \cdot 9)/4 = –6$
…
$k = –6 \rightarrow x = (3 – 6 \cdot 9)/4 = –15$
…

Nilai-nilai *x* yang memenuhi: 3, 12, … dan –6, –15, …

(ii) $2x \equiv 3 \pmod 4$

$$x = \frac{3 + k \cdot 4}{2}$$

Karena $4k$ genap dan 3 ganjil maka penjumlahannya menghasilkan ganjil, sehingga hasil penjumlahan tersebut jika dibagi dengan 2 tidak menghasilkan bilangan bulat. Dengan kata lain, tidak ada nilai-nilai x yang memenuhi $2x \equiv 3 \pmod 4$.

Chinese Remainder Problem

Pada abad pertama, seorang matematikawan China yang bernama Sun Tse mengajukan pertanyaan sebagai berikut:

> *Tentukan sebuah bilangan bulat yang bila dibagi dengan 5 menyisakan 3, bila dibagi 7 menyisakan 5, dan bila dibagi 11 menyisakan 7.*

Pertanyaan Sun Tse dapat dirumuskan kedalam sistem kongruen lanjar:

$$x \equiv 3 \pmod 5$$
$$x \equiv 5 \pmod 7$$
$$x \equiv 7 \pmod{11}$$

TEOREMA 5.6. (*Chinese Remainder Theorem*) Misalkan m_1, m_2, …, m_n adalah bilangan bulat positif sedemikian sehingga PBB(m_i, m_j) = 1 untuk $i \neq j$. Maka sistem kongruen lanjar

$$x \equiv a_k \pmod{m_k}$$

mempunyai sebuah solusi unik modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

Contoh 14.
Tentukan solusi dari pertanyaan Sun Tse di atas.

Penyelesaian:
Menurut persamaan (5.6), kongruen pertama, $x \equiv 3 \pmod 5$, memberikan $x = 3 + 5k_1$ untuk beberapa nilai k. Sulihkan ini ke dalam kongruen kedua menjadi $3 + 5k_1 \equiv 5 \pmod 7$, dari sini kita peroleh $k_1 \equiv 6 \pmod 7$, atau $k_1 = 6 + 7k_2$ untuk beberapa nilai k_2. Jadi kita mendapatkan $x = 3 + 5k_1 = 3 + 5(6 + 7k_2) = 33 + 35k_2$ yang mana memenuhi dua kongruen pertama. Jika x memenuhi kongruen yang ketiga, kita harus mempunyai $33 + 35k_2 \equiv 7 \pmod{11}$, yang mengakibatkan $k_2 \equiv 9 \pmod{11}$ atau $k_2 = 9 + 11k_3$. Sulihkan k_2 ini ke dalam kongruen yang ketiga menghasilkan $x = 33 + 35(9 + 11k_3) \equiv 348 + 385k_3 \pmod{11}$. Dengan demikian, $x \equiv 348 \pmod{385}$ yang memenuhi ketiga konruen tersebut. Dengan kata lain, 348 adalah solusi unik modulo 385. Catatlah bahwa $385 = 5 \cdot 7 \cdot 11$.

Solusi unik ini mudah dibuktikan sebagai berikut. Solusi tersebut modulo $m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 7 \cdot 11 = 5 \cdot 77 = 11 \cdot 35$. Karena $77\ 3 \equiv 1 \pmod 5$, $55 \cdot 6 \equiv 1 \pmod 7$, dan $35 \cdot 6 \equiv 1 \pmod{11}$, solusi unik dari sistem kongruen tersebut adalah

$$\begin{aligned} x &\equiv 3 \cdot 77 \cdot 3 + 5 \cdot 55 \cdot 6 + 7 \cdot 35 \cdot 6 \pmod{385} \\ &\equiv 3813 \pmod{385} \equiv 348 \pmod{385} \end{aligned}$$

3.5 Aritmetika Modulo dan Kriptografi

Aritmetika modulo cocok digunakan untuk kriptografi karena dua alasan:

1. Oleh karena nilai-nilai aritmetika modulo berada dalam himpunan berhingga (0 sampai modulus $m - 1$), maka kita tidak perlu khawatir hasil perhitungan berada di luar himpunan.

2. Karena kita bekerja dengan bilangan bulat, maka kita tidak khawatir kehilangan informasi akibat pembulatan (*round off*) sebagaimana pada operasi bilangan riil.

3.6 Bilangan Prima

- Bilangan bulat positif p ($p > 1$) disebut bilangan prima jika pembaginya hanya 1 dan p.

- Contoh: 23 adalah bilangan prima karena ia hanya habis dibagi oleh 1 dan 23.

- Karena bilangan prima harus lebih besar dari 1, maka barisan bilangan prima dimulai dari 2, yaitu 2, 3, 5, 7, 11, 13, …. Seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap.

- Bilangan selain prima disebut bilangan **komposit** (*composite*). Misalnya 20 adalah bilangan komposit karena 20 dapat dibagi oleh 2, 4, 5, dan 10, selain 1 dan 20 sendiri.

Teorema 3. (*The Fundamental Theorem of Arithmetic*). Setiap bilangan bulat positif yang lebih besar atau sama dengan 2 dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima.

Contoh 15.

$9 = 3 \times 3$ (2 buah faktor prima)
$100 = 2 \times 2 \times 5 \times 5$ (4 buah faktor prima)
$13 = 13$ (atau 1×13) (1 buah faktor prima)

- Untuk menguji apakah *n* merupakan bilangan prima atau komposit, kita cukup membagi *n* dengan sejumlah bilangan prima, mulai dari 2, 3, … , bilangan prima $\leq \sqrt{n}$. Jika *n* habis dibagi dengan salah satu dari bilangan prima tersebut, maka *n* adalah bilangan komposit, tetapi jika *n* tidak habis dibagi oleh semua bilangan prima tersebut, maka n adalah bilangan prima.

Contoh 16.

Tunjukkan apakah (i) 171 dan (ii) 199 merupakan bilangan prima atau komposit.

Penyelesaian*:*

(i) $\sqrt{171} = 13.077$. Bilangan prima yang $\leq \sqrt{171}$ adalah 2, 3, 5, 7, 11, 13. Karena 171 habis dibagi 3, maka 171 adalah bilangan komposit.

(ii) $\sqrt{199} = 14.107$. Bilangan prima yang $\leq \sqrt{199}$ adalah 2, 3, 5, 7, 11, 13. Karena 199 tidak habis dibagi 2, 3, 5, 7, 11, dan 13, maka 199 adalah bilangan prima.

- Terdapat metode lain yang dapat digunakan untuk menguji keprimaan suatu bilangan bulat, yang terkenal dengan **Teorema Fermat**. Fermat (dibaca “Fair-ma”) adalah seorang matematikawan Perancis pada tahun 1640.

Teorema 4 (**Teorema Fermat**). Jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi dengan p, yaitu PBB(a, p) = 1, maka

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

Contoh 17.
Kita akan menguji apakah 17 dan 21 bilangan prima atau bukan. Di sini kita mengambil nilai a = 2 karena PBB(17, 2) = 1 dan PBB(21, 2) = 1. Untuk 17,

$$2^{17-1} = 65536 \equiv 1 \pmod{17}$$

karena 17 tidak membagi 65536 – 1 = 65535 (65535 ÷ 17 = 3855). Untuk 21,

$$2^{21-1} = 1048576 \not\equiv 1 \pmod{21}$$

karena 21 tidak habis membagi 1048576 – 1 = 1048575.

- Kelemahan Teorema Fermat: terdapat bilangan komposit n sedemikian sehingga $2^{n-1} \equiv 1 \pmod{n}$. Bilangan bulat seperti itu disebut bilangan **prima semu** (*pseudoprimes*).

- Misalnya komposit 341 (yaitu 341 = 11 · 31) adalah bilangan prima semu karena menurut teorema Fermat,

  $$2^{340} \equiv 1 \pmod{341}$$

  Untunglah bilangan prima semu relatif jarang terdapat.

Fungsi Euler f

- Fungsi Euler ϕ medefinisikan $\phi(n)$ untuk $n \geq 1$ yang menyatakan jumlah bilangan bulat positif < n yang relatif prima dengan n.

Contoh 18
Tentukan $\phi(20)$.

Penyelesaian:
Bilangan bulat positif yang lebih kecil dari 20 adalah 1 sampai 19. Di antara bilangan-bilangan tersebut, terdapat $\phi(20) = 8$ buah yang relatif prima dengan 20, yaitu 1, 3, 7, 9, 11, 13, 17, 19.

Untuk n = 1, 2, …, 10, fungsi Euler adalah

$\phi(1) = 0$	$\phi(6) = 2$
$\phi(2) = 1$	$\phi(7) = 6$
$\phi(3) = 2$	$\phi(8) = 4$
$\phi(4) = 2$	$\phi(9) = 6$
$\phi(5) = 4$	$\phi(10) = 4$

- Jika n prima, maka setiap bilangan bulat yang lebih kecil dari n relatif prima terhadap n. Dengan kata lain, $\phi(n) = n - 1$ hanya jika n prima.

Contoh 19
$\phi(3) = 2$, $\phi(5) = 4$, $\phi(7) = 6$, $\phi(11) = 10$, $\phi(13) = 12$, dst.

Teorema 5. Jika $n = pq$ adalah bilangan komposit dengan p dan q prima, maka $\phi(n) = \phi(p)\,\phi(q) = (p-1)(q-1)$.

Contoh 20.
Tentukan $\phi(21)$.

Penyelesaian:
Karena $21 = 7 \cdot 3$, $\phi(21) = \phi(7)\,\phi(3) = 6 \cdot 2 = 12$ buah bilangan bulat yang relatif prima terhadap 21, yaitu 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20.

Teorema 6. Jika p bilangan prima dan $k > 0$, maka $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Contoh 22.
Tentukan $\phi(16)$.

Penyelesaian:
Karena $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$, maka ada delapan buah bilangan bulat yang relatif prima terhadap 16, yaitu 1, 3, 5, 7, 9, 11, 13, 15.

Teorema 7 (*Euler's generalization of Fermat theorem*). Jika PBB(a, n) = 1, maka

$$a^{\phi(n)} \bmod n = 1 \qquad (\text{atau } a^{\phi(n)} \equiv 1 \pmod{n})$$