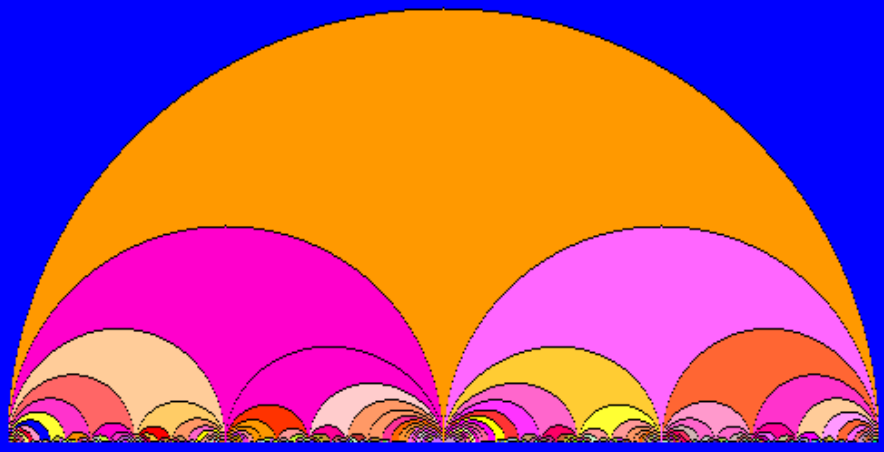


Satu Lagi
Buku Teks Pengantar
Teori Bilangan

(Versi dengan Penekanan pada Kriptologi)

Jonathan A. Poritz

berdasarkan karya Wissam Raji

Departemen Matematika dan Fisika
Colorado State University, Pueblo
2200 Bonforte Blvd.
Pueblo, CO 81001, USA
Surel: jonathan.poritz@gmail.com
Situs web: www.poritz.net/jonathan

07 Mei 2014 11:04 MDT

Prakata

Ini adalah draf pertama sebuah buku ajar teori bilangan tingkat sarjana yang bebas (dalam arti kebebasan berbicara, bukan gratis seperti bir gratis, [**Sta02**]), meskipun buku ini juga tersedia secara gratis. Buku ini digunakan dalam mata kuliah Math 319 di Colorado State University – Pueblo pada semester musim semi 2014. Ucapan terima kasih disampaikan kepada para mahasiswa di kelas tersebut – Megan Bissell, Tennille Candelaria, Ariana Carlyle, Michael Degraw, Daniel Fisher, Aaron Griffin, Lindsay Harder, Graham Harper, Helen Huang, Daniel Nichols, dan Arika Waldrep – yang memberikan banyak saran berguna dan menemukan banyak salah ketik. Saya juga berterima kasih kepada para mahasiswa dalam mata kuliah Math 242 Pengantar Pemrograman Matematika pada semester musim semi 2014 yang sama – Stephen Ciruli, Jamen Cox, Graham Harper, Joel Kienitz, Matthew Klamm, Christopher Martin, Corey Sullinger, James Todd, dan Shelby Whalen – karena berbagai proyek pemrograman mereka menghasilkan kode yang saya adaptasi untuk membuat beberapa gambar dan contoh dalam buku ini.

Penulis menyampaikan penghargaan dan terima kasih atas karya **An Introductory Course in Elementary Number Theory** oleh Wissam Raji [lihat Saylor Academy], yang menjadi sumber adaptasi awal buku ini. Karya Raji diterbitkan dengan lisensi Creative Commons **CC BY 3.0** , lihat ketentuan CC BY 3.0. Karya ini diterbitkan dengan lisensi **CC BY-SA 4.0**, lihat ketentuan CC BY-SA 4.0. Perbedaannya adalah bahwa jika Anda membangun karya baru berdasarkan karya ini, karya turunan tersebut juga harus diterbitkan dengan lisensi yang mengizinkan orang lain membuat adaptasi lebih lanjut yang tidak Anda kendalikan.

Catatan edisi bahasa Indonesia: Edisi ini adalah terjemahan dan adaptasi bahasa Indonesia yang dibuat dari sumber Jonathan A. Poritz bertanda waktu 7 Mei 2014 11:04 MDT. Perubahan bahasa dan teknis dicatat dalam manifes edisi. Edisi ini bukan terbitan resmi dari Jonathan A. Poritz, Wissam Raji, atau Colorado State University – Pueblo dan tidak menyiratkan dukungan mereka. Edisi turunan ini tetap menggunakan lisensi CC BY-SA 4.0.

Versi sumber: 07 Mei 2014 11:04 MDT. Perhatikan bahwa penulis akan sering memperbarui dan menyempurnakan teks ini jika waktu memungkinkan, khususnya selama dan segera setelah semester ketika buku ini digunakan dalam perkuliahan. Karena itu, silakan sering memeriksa situs resmi buku ini.

Karya ini dipersembahkan kepada rekan-rekan saya di Colorado State University – Pueblo yang bekerja luar biasa keras. Dedikasi mereka kepada mahasiswa, kegiatan ilmiah, dan komunitas mereka merupakan sumber inspirasi. Ketika saya mengerjakan versi pertama buku ini, rekan-rekan tersebut melawan omong kosong administratif yang sangat picik dan bebal, termasuk yang terburuk yang pernah saya saksikan selama lebih dari tiga puluh tahun berkecimpung dalam pendidikan tinggi. Seperti dikatakan MLK, "Busur alam semesta moral itu panjang, tetapi melengkung ke arah keadilan." Kerja keras kalian—yang cerdas dan tanpa pamrih—membuatnya melengkung.

Jonathan A. Poritz, 7 Mei 2014, Pueblo, CO, AS

Catatan Rilis

Versi *YAINTT* ini memberikan penekanan khusus pada hubungan dengan kriptologi. Materi kriptologi terdapat dalam Bab 4 serta §§ 5.5 dan 5.6; materi tersebut muncul secara alami (demikian harapan saya) dari teori bilangan yang melingkupinya. Aplikasi utama kriptologi – yaitu kriptosistem RSA, pertukaran kunci Diffie–Hellman, dan kriptosistem ElGamal – muncul begitu alami dari pembahasan Teorema Euler, akar primitif, dan indeks sehingga pernyataan G.H. Hardy [**Har05**] mengenai kemurnian dan ketakterterapan abadi teori bilangan menjadi cukup ironis.

Namun, setelah mulai membahas algoritma kriptologi tersebut, kita meluangkan waktu untuk mendefinisikan banyak konsep kriptologi secara cermat dan mengembangkan beberapa gagasan terkait yang hubungannya dengan teori bilangan jauh lebih longgar. Karena itu, materi ini terasa agak berbeda dari bagian lain buku – sebagaimana semua karya ilmiah dalam kriptologi (dan mungkin dalam seluruh ilmu komputer), suatu disiplin yang jelas memiliki budaya berbeda dari matematika "murni". Bagian-bagian tersebut tentu dapat dilewati oleh pembaca yang tidak berminat, atau dihapus oleh pengajar ketika meramu buku ini sesuai pendekatan kelasnya.

Perhatian: Sebagaimana lazimnya dalam gaya Bourbaki[1], kemunculan simbol ini dalam teks menandai bagian dengan penalaran yang rumit dan sulit diikuti, atau mengingatkan pembaca pada kesalahpahaman umum mengenai suatu hal.

Versi sumber dalam format PDF tersedia melalui tautan PDF resmi, sedangkan seluruh berkas untuk membuat versi khusus tersedia melalui direktori sumber resmi – silakan berkreasi; itulah tujuan Creative Commons!

[1]Seorang matematikawan fiktif dan penulis banyak buku matematika bermutu yang tidak fiktif – buku-buku itu benar-benar ada – seperti [**Bou04**]

Daftar Isi

BAB 1

Keterurutan Baik dan Pembagian

1.1. Prinsip Keterurutan Baik dan Induksi Matematika

Dalam bab ini, kita menyajikan tiga alat dasar yang akan sering digunakan untuk membuktikan sifat-sifat bilangan bulat. Kita mulai dengan sebuah sifat bilangan bulat yang sangat penting, yaitu prinsip keterurutan baik. Selanjutnya, kita menyatakan apa yang dikenal sebagai prinsip sarang merpati, lalu memperkenalkan metode penting yang disebut induksi matematika.

1.1.1. Prinsip Keterurutan Baik.

DEFINISI 1.1.1. Diberikan suatu himpunan bilangan S (dari jenis apa pun), kita mengatakan bahwa $\ell \in S$ adalah **elemen terkecil dari** S jika $\forall x \in S$, berlaku $x = \ell$ atau $\ell < x$.

PRINSIP KETERURUTAN BAIK. Setiap himpunan bilangan asli yang tidak kosong memiliki elemen terkecil.

Prinsip ini sering diambil sebagai sebuah aksioma.

1.1.2. Prinsip Sarang Merpati.

TEOREMA 1.1.2. ***Prinsip Sarang Merpati:*** *Misalkan $s, k \in \mathbb{N}$ memenuhi $s > k$. Jika s objek ditempatkan ke dalam k kotak, maka sekurang-kurangnya satu kotak memuat lebih dari satu objek.*

BUKTI. Andaikan setiap kotak memuat paling banyak satu objek. Maka terdapat paling banyak k objek, padahal terdapat s objek dengan $s > k$. □

1.1.3. Prinsip Induksi Matematika. Sekarang kita menyajikan sebuah alat berharga untuk membuktikan hasil-hasil mengenai bilangan bulat. Alat ini adalah prinsip induksi matematika.

TEOREMA 1.1.3. ***Prinsip Pertama Induksi Matematika:*** *Misalkan $S \subset \mathbb{N}$ adalah himpunan yang memenuhi kedua sifat berikut:*

(1) $1 \in S$*; dan*
(2) $\forall k \in \mathbb{N},\ k \in S \Rightarrow k + 1 \in S$.

Maka $S = \mathbb{N}$.
Secara lebih umum, misalkan $\mathcal{P}(n)$ *adalah suatu sifat bilangan asli yang mungkin benar atau mungkin tidak benar untuk suatu* $n \in \mathbb{N}$ *tertentu, dan memenuhi*

(1) $\mathcal{P}(1)$ *benar; dan*
(2) $\forall k \in \mathbb{N},\ \mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$

maka $\forall n \in \mathbb{N}, \mathcal{P}(n)$ *benar.*

BUKTI. Kita menggunakan prinsip keterurutan baik untuk membuktikan prinsip pertama induksi matematika ini.

Misalkan S adalah himpunan pada bagian pertama teorema dan T adalah himpunan bilangan asli yang tidak termasuk dalam S. Kita akan menggunakan bukti dengan kontradiksi, jadi andaikan T tidak kosong.

Menurut prinsip keterurutan baik, T memiliki elemen terkecil ℓ.

Perhatikan bahwa $1 \in S$, sehingga $1 \notin T$ dan akibatnya $\ell > 1$. Jadi, $\ell - 1$ adalah bilangan asli. Karena ℓ merupakan elemen terkecil dari T, maka $\ell - 1$ tidak berada di T; oleh karena itu, bilangan tersebut berada di S.

Namun, berdasarkan sifat yang mendefinisikan S, karena $\ell - 1 \in S$, kita memperoleh $\ell = \ell - 1 + 1 \in S$. Hal ini bertentangan dengan fakta bahwa ℓ adalah elemen terkecil dari T, sehingga berada di T dan tidak berada di S.

Kontradiksi ini menunjukkan bahwa anggapan bahwa T tidak kosong adalah salah; dengan demikian, $S = \mathbb{N}$.

Untuk bagian kedua teorema, ambil $S = \{n \in \mathbb{N} \mid \mathcal{P}(n) \text{ benar}\}$, lalu terapkan bagian pertama. □

CONTOH 1.1.4. Kita menggunakan induksi matematika untuk menunjukkan bahwa $\forall n \in \mathbb{N}$,

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}. \tag{1.1.1}$$

Pertama, perhatikan bahwa

$$\sum_{j=1}^{1} j = 1 = \frac{1 \cdot 2}{2}$$

sehingga pernyataan tersebut benar untuk $n = 1$. Untuk langkah induksi selanjutnya, andaikan rumus itu berlaku bagi suatu $n \in \mathbb{N}$ tertentu, yaitu $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$. Kita tunjukkan bahwa

$$\sum_{j=1}^{n+1} j = \frac{(n+1)(n+2)}{2}.$$

Dengan demikian, bukti induksi akan lengkap. Memang,

$$\sum_{j=1}^{n+1} j = \sum_{j=1}^{n} j + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

dan hasil yang diinginkan pun diperoleh.

CONTOH 1.1.5. Sekarang kita menggunakan induksi matematika untuk membuktikan bahwa $n! \leq n^n$ untuk setiap $n \in \mathbb{N}$.

Perhatikan bahwa $1! = 1 \leq 1^1 = 1$. Selanjutnya, kita menyajikan langkah induksi. Andaikan

$$n! \leq n^n$$

untuk suatu $n \in \mathbb{N}$. Kita buktikan bahwa $(n+1)! \leq (n+1)^{n+1}$. Perhatikan bahwa

$$(n+1)! = (n+1)n! \leq (n+1) \cdot n^n < (n+1)(n+1)^n = (n+1)^{n+1}.$$

Ini melengkapi bukti.

TEOREMA 1.1.6. ***Prinsip Kedua Induksi Matematika:*** *Misalkan $S \subset \mathbb{N}$ adalah himpunan yang memenuhi kedua sifat berikut:*

(1) $1 \in S$*; dan*

(2) $\forall k \in \mathbb{N},\ 1, \ldots, k \in S \Rightarrow k+1 \in S$.

Maka $S = \mathbb{N}$.

Secara lebih umum, misalkan $\mathcal{P}(n)$ adalah suatu sifat bilangan asli yang mungkin benar atau mungkin tidak benar untuk suatu $n \in \mathbb{N}$ tertentu, dan memenuhi

(1) $\mathcal{P}(1)$ *benar; dan*

(2) $\forall k \in \mathbb{N}$, *jika* $\mathcal{P}(1), \ldots, \mathcal{P}(k)$ *semuanya benar, maka* $\mathcal{P}(k+1)$ *juga benar,*

maka $\forall n \in \mathbb{N}, \mathcal{P}(n)$ *benar.*

BUKTI. Untuk membuktikan prinsip kedua induksi, kita menggunakan prinsip pertama induksi.

Misalkan S adalah himpunan bilangan bulat seperti pada bagian pertama teorema. Untuk $n \in \mathbb{N}$, misalkan $\mathcal{P}(n)$ adalah sifat matematika "$1, \ldots, n \in S$". Kita dapat menerapkan Prinsip Pertama Induksi Matematika untuk membuktikan bahwa $\forall n \in \mathbb{N}\ \mathcal{P}(n)$ benar, yang berarti $S = \mathbb{N}$. *[Rinciannya diserahkan kepada pembaca.]*

Bagian kedua teorema mengikuti bagian pertama dengan cara yang persis sama seperti bagian kedua Prinsip Pertama Induksi Matematika mengikuti bagian pertamanya. □

Latihan untuk §1.1.

LATIHAN 1.1.1. Buktikan dengan induksi matematika bahwa $n < 3^n$ untuk setiap bilangan bulat positif n.

LATIHAN 1.1.2. Tunjukkan bahwa $\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$.

LATIHAN 1.1.3. Gunakan induksi matematika untuk membuktikan bahwa $\sum_{j=1}^{n}(-1)^{j-1}j^2 = (-1)^{n-1}n(n+1)/2$.

LATIHAN 1.1.4. Gunakan induksi matematika untuk membuktikan bahwa $\sum_{j=1}^{n} j^3 = [n(n+1)/2]^2$ untuk setiap bilangan bulat positif n.

LATIHAN 1.1.5. Gunakan induksi matematika untuk membuktikan bahwa $\sum_{j=1}^{n}(2j-1) = n^2$.

LATIHAN 1.1.6. Gunakan induksi matematika untuk membuktikan bahwa $2^n < n!$ untuk $n \geq 4$.

LATIHAN 1.1.7. Gunakan induksi matematika untuk membuktikan bahwa $n^2 < n!$ untuk $n \geq 4$.

1.2. Operasi Aljabar pada Bilangan Bulat

Pada $\mathbb{Z}$, himpunan bilangan bulat, terdapat dua operasi biner dasar, yaitu **penjumlahan** (dinotasikan dengan $+$) dan **perkalian** (dinotasikan dengan $\cdot$). Kedua operasi ini memenuhi sifat-sifat yang sudah dikenal berikut:

(1) **Komutativitas penjumlahan dan perkalian**

$$\forall a, b \in \mathbb{Z}: \quad a + b = b + a$$
$$a \cdot b = b \cdot a$$

(2) **Asosiativitas penjumlahan dan perkalian**

$$\forall a, b, c \in \mathbb{Z}: \quad (a + b) + c = a + (b + c)$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(3) **Distributivitas perkalian terhadap penjumlahan**

$$\forall a, b, c \in \mathbb{Z}: \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$

Di dalam himpunan $\mathbb{Z}$ terdapat *elemen identitas* untuk kedua operasi $+$ dan $\cdot$, masing-masing yaitu elemen 0 dan 1. Elemen-elemen ini memenuhi sifat dasar

$$\forall a \in \mathbb{Z}: \quad a + 0 = 0 + a = a$$
$$a \cdot 1 = 1 \cdot a = a\,.$$

Setiap elemen dalam himpunan $\mathbb{Z}$ mempunyai **invers aditif**. Artinya, untuk setiap $a \in \mathbb{Z}$ terdapat bilangan bulat lain dalam $\mathbb{Z}$, yang dinotasikan dengan $-a$, sedemikian sehingga

$$a + (-a) = 0. \tag{1.2.1}$$

Untuk perkalian, bilangan bulat yang mempunyai **invers multiplikatif** hanyalah 1 dan -1. Untuk kedua bilangan tersebut, invers multiplikatif yang dinotasikan dengan a^{-1} atau $1/a$ sama dengan a itu sendiri, sehingga

$$a \cdot a^{-1} = 1. \tag{1.2.2}$$

Dari operasi penjumlahan dan perkalian, kita dapat mendefinisikan dua operasi lain pada $\mathbb{Z}$, yaitu **pengurangan** (dinotasikan dengan $-$) dan **pembagian** (dinotasikan dengan $/$). Pengurangan merupakan operasi biner pada $\mathbb{Z}$, yakni didefinisikan untuk setiap pasangan bilangan bulat dalam $\mathbb{Z}$. Sebaliknya, pembagian bukan operasi biner pada $\mathbb{Z}$ sehingga hanya didefinisikan untuk pasangan bilangan bulat tertentu. Pengurangan dan pembagian didefinisikan sebagai berikut:

(1) $\forall a, b \in \mathbb{Z}$, $a - b$ didefinisikan sebagai $a + (-b)$.
(2) Diberikan $a, b \in \mathbb{Z}$ dengan $b \neq 0$. Jika $\exists c \in \mathbb{Z}$ sedemikian sehingga $a = b \cdot c$, maka a/b didefinisikan sebagai c.

1.3. Keterbagian dan Algoritma Pembagian

Sekarang kita membahas konsep keterbagian beserta sifat-sifatnya.

1.3.1. Keterbagian Bilangan Bulat.

DEFINISI 1.3.1. Jika a dan b adalah bilangan bulat dengan $a \neq 0$, kita mengatakan bahwa a **membagi** b dan menulis $a \mid b$ apabila terdapat bilangan bulat k sedemikian sehingga $b = ka$. Dengan kata lain, untuk $a, b \in \mathbb{Z}$ dengan $a \neq 0$, kita menulis $a \mid b$ apabila $\exists k \in \mathbb{Z}$ sedemikian sehingga $b = ka$.

Jika a membagi b, kita juga mengatakan bahwa a adalah **faktor** [atau **pembagi**] dari b, dan bahwa b adalah **kelipatan** dari a. Jika a tidak membagi b, kita menulis $a \nmid b$.

CONTOH 1.3.2. Sebagai contoh, $2 \mid 4$ dan $7 \mid 63$, sedangkan $5 \nmid 26$.

DEFINISI 1.3.3. Untuk $a \in \mathbb{Z}$, kita mengatakan bahwa a adalah bilangan **genap** jika $2 \mid a$, yaitu jika $\exists k \in \mathbb{Z}$ sedemikian sehingga $a = 2k$. Sebaliknya, untuk $a \in \mathbb{Z}$, kita mengatakan bahwa a adalah bilangan **ganjil** jika $2 \nmid a$.

Sebagai konsekuensi dari Algoritma Pembagian di bawah ini, jika a ganjil maka $\exists k \in \mathbb{Z}$ sedemikian sehingga $a = 2k + 1$.

PROPOSISI 1.3.4. *Untuk setiap $a \in \mathbb{Z} \setminus \{0\}$ berlaku $a \mid 0$.*

PROPOSISI 1.3.5. *Jika $a, b \in \mathbb{Z}$ memenuhi $|b| < a$ dan $b \neq 0$, maka $a \nmid b$.*

PROPOSISI 1.3.6. *Untuk $a, b \in \mathbb{Z}$ dengan $a \neq 0$, berlaku $a \mid b \Leftrightarrow a \mid |b|$.*

TEOREMA 1.3.7. *Jika a, b, dan c adalah bilangan bulat yang memenuhi $a \mid b$ dan $b \mid c$, maka $a \mid c$.*

BUKTI. Karena $a \mid b$ dan $b \mid c$, terdapat $k_1, k_2 \in \mathbb{Z}$ sedemikian sehingga $b = k_1 a$ dan $c = k_2 b$. Oleh karena itu, $c = k_1 k_2 a$, sehingga $a \mid c$. □

CONTOH 1.3.8. Karena $6 \mid 18$ dan $18 \mid 36$, maka $6 \mid 36$.

Teorema berikut menyatakan bahwa jika suatu bilangan bulat membagi dua bilangan bulat lain, bilangan tersebut juga membagi setiap kombinasi linear keduanya.

TEOREMA 1.3.9. *Untuk setiap $a, b, c, m, n \in \mathbb{Z}$, jika $c \mid a$ dan $c \mid b$, maka $c \mid (ma+nb)$.*

BUKTI. Karena $c \mid a$ dan $c \mid b$, terdapat $k_1, k_2 \in \mathbb{Z}$ sedemikian sehingga $a = k_1 c$ dan $b = k_2 c$. Dengan demikian,

$$ma + nb = mk_1 c + nk_2 c = c(mk_1 + nk_2),$$

dan karena itu $c \mid (ma + nb)$. □

Teorema 1.3.9 dapat diperumum ke setiap kombinasi linear berhingga sebagai berikut. Jika

$$n \in \mathbb{N},\ a, b_1, \ldots, b_n \in \mathbb{Z} \text{ dan } a \mid b_1, a \mid b_2, \ldots, a \mid b_n,$$

maka, untuk setiap $k_1, \ldots, k_n \in \mathbb{Z}$,

$$a \mid \sum_{j=1}^{n} k_j b_j \tag{1.3.1}$$

Pembuktian perumuman ini dengan induksi merupakan latihan yang baik.

1.3.2. Algoritma Pembagian.

TEOREMA 1.3.10. ***Algoritma Pembagian*** *Diberikan $a, b \in \mathbb{Z}$ dengan $b > 0$, terdapat pasangan tunggal $q, r \in \mathbb{Z}$ sedemikian sehingga $a = qb + r$ dan $0 \leq r < b$. Bilangan q disebut* **hasil bagi***, sedangkan r disebut* **sisa pembagian** *a* **oleh** *b.*

BUKTI. Perhatikan himpunan $A = \{a - bk \mid k \in \mathbb{Z},\ a - bk \geq 0\}$. Himpunan A tidak kosong karena untuk $k < a/b$ berlaku $a - bk > 0$. Menurut prinsip keterurutan baik, A memiliki elemen terkecil $r = a - qb$ untuk suatu $q \in \mathbb{Z}$. Berdasarkan konstruksinya, $r \geq 0$. Sekarang, jika $r \geq b$, maka (karena $b > 0$)

$$r > r - b = a - qb - b = a - (q + 1)b \geq 0.$$

Hal ini menghasilkan kontradiksi karena r diasumsikan sebagai elemen terkecil A. Oleh karena itu, $0 \leq r < b$.

Selanjutnya kita tunjukkan bahwa q dan r tunggal. Misalkan $a = q_1 b + r_1$ dan $a = q_2 b + r_2$, dengan $0 \leq r_1 < b$ dan $0 \leq r_2 < b$. Maka

$$a - a = q_1 b + r_1 - (q_2 b + r_2) = (q_1 - q_2)b + (r_1 - r_2) = 0.$$

Akibatnya,

$$(q_1 - q_2)b = r_2 - r_1.$$

Jadi,

$$b \mid (r_2 - r_1).$$

Karena $0 \leq |r_2 - r_1| \leq \max(r_1, r_2)$ dan $b > \max(r_1, r_2)$, maka $r_2 - r_1$ harus sama dengan 0, yaitu $r_2 = r_1$. Karena $bq_1 + r_1 = bq_2 + r_2$, kita juga memperoleh $q_1 = q_2$. Hal ini membuktikan ketunggalan. □

CONTOH 1.3.11. Jika $a = 71$ dan $b = 6$, maka $71 = 6 \cdot 11 + 5$. Di sini $q = 11$ dan $r = 5$.

Latihan untuk §1.3.

LATIHAN 1.3.1. Tunjukkan bahwa $5 \mid 25$, $19 \mid 38$, dan $2 \mid 98$.

LATIHAN 1.3.2. Gunakan Algoritma Pembagian untuk menentukan hasil bagi dan sisa ketika 76 dibagi oleh 13.

LATIHAN 1.3.3. Gunakan Algoritma Pembagian untuk menentukan hasil bagi dan sisa ketika -100 dibagi oleh 13.

LATIHAN 1.3.4. Tunjukkan bahwa jika a, b, c, dan d adalah bilangan bulat, dengan a dan c tidak nol, serta $a \mid b$ dan $c \mid d$, maka $ac \mid bd$.

LATIHAN 1.3.5. Tunjukkan bahwa jika a dan b adalah bilangan bulat positif dan $a \mid b$, maka $a \leq b$.

LATIHAN 1.3.6. Buktikan bahwa jumlah dua bilangan bulat genap adalah genap, jumlah dua bilangan bulat ganjil adalah genap, dan jumlah sebuah bilangan bulat genap dengan sebuah bilangan bulat ganjil adalah ganjil.

LATIHAN 1.3.7. Tunjukkan bahwa hasil kali dua bilangan bulat genap adalah genap, hasil kali dua bilangan bulat ganjil adalah ganjil, dan hasil kali sebuah bilangan bulat genap dengan sebuah bilangan bulat ganjil adalah genap.

LATIHAN 1.3.8. Tunjukkan bahwa jika m adalah bilangan bulat, maka 3 membagi $m^3 - m$.

LATIHAN 1.3.9. Tunjukkan bahwa kuadrat setiap bilangan bulat ganjil berbentuk $8m + 1$ untuk suatu $m \in \mathbb{Z}$.

LATIHAN 1.3.10. Tunjukkan bahwa untuk setiap bilangan bulat n, kuadrat n berbentuk $3m$ atau $3m + 1$ untuk suatu $m \in \mathbb{Z}$, tetapi tidak pernah berbentuk $3m + 2$ untuk $m \in \mathbb{Z}$.

LATIHAN 1.3.11. Tunjukkan bahwa jika $ac \mid bc$, maka $a \mid b$.

LATIHAN 1.3.12. Tunjukkan bahwa jika $a \mid b$ dan $b \mid a$, maka $a = \pm b$.

1.4. Representasi Bilangan Bulat dalam Berbagai Basis

Pada bagian ini, kita menunjukkan bahwa setiap bilangan bulat positif dapat dituliskan secara unik dalam ekspansi pada sebarang basis bilangan bulat yang lebih besar dari 1. Biasanya kita menggunakan notasi desimal untuk merepresentasikan bilangan bulat. Kita akan menunjukkan cara mengubah bilangan bulat dari notasi desimal ke notasi dengan sebarang basis bilangan bulat lain, dan sebaliknya. Notasi desimal mungkin menjadi tradisi dalam kehidupan sehari-hari semata-mata karena kita memiliki sepuluh jari tangan. ("Lalu bagaimana dengan jari kaki kita?" protes Anda. Saya tidak tahu. Dan tampaknya bangsa Babilonia memiliki 30 jari pada setiap tangan, atau 15 jari pada setiap tangan dan kaki, sebab mereka menggunakan basis 60.)

Notasi Bilangan bulat a yang ditulis dalam ekspansi basis b dilambangkan dengan $(a)_b$.

TEOREMA 1.4.1. *Misalkan $b \in \mathbb{Z}$ memenuhi $b > 1$. Maka, untuk setiap $m \in \mathbb{N}$, terdapat tepat satu $l \in \mathbb{Z}_{\geq 0}$ beserta digit-digit $a_0, a_1, \ldots, a_l \in \mathbb{Z}$ sedemikian sehingga*

$$m = \sum_{j=0}^{l} a_j b^j,$$

$$0 \leq a_j < b \text{ untuk } j = 0, 1, \ldots, l, \text{ dan}$$

$$a_l \neq 0.$$

BUKTI. Ambil sebarang $m \in \mathbb{N}$. Mula-mula kita membagi m dengan b menggunakan Algoritma Pembagian, sehingga diperoleh

$$m = q_0 b + a_0, \quad 0 \leq a_0 < b.$$

Jika $q_0 \neq 0$, selanjutnya kita membagi q_0 dengan b dan memperoleh

$$q_0 = q_1 b + a_1, \quad 0 \leq a_1 < b.$$

Jika $q_0 = 0$, ambil $l = 0$ dan $a_0 = m$; bagian eksistensi selesai. Selanjutnya, anggap $q_0 > 0$. Karena setiap hasil bagi positif berikutnya lebih kecil daripada hasil bagi sebelumnya, untuk suatu $l \geq 1$ proses ini pertama kali berakhir pada $q_l = 0$. Dengan demikian,

$$\begin{aligned} q_{j-1} &= q_j b + a_j, \qquad 0 \leq a_j < b \quad (j = 1, \ldots, l), \\ q_l &= 0, \qquad a_l = q_{l-1} \neq 0. \end{aligned}$$

Sekarang, dengan menyubstitusikan persamaan $q_0 = q_1 b + a_1$ ke dalam $m = q_0 b + a_0$, diperoleh

$$m = (q_1 b + a_1) b + a_0 = q_1 b^2 + a_1 b + a_0.$$

Dengan menyubstitusikan persamaan-persamaan tersebut secara berturut-turut (atau dengan induksi pada j), diperoleh

$$\begin{aligned} m &= q_{j-1}b^j + \sum_{i=0}^{j-1} a_i b^i \qquad (j = 1, \ldots, l), \\ &= a_l b^l + \sum_{i=0}^{l-1} a_i b^i = \sum_{i=0}^{l} a_i b^i. \end{aligned}$$

Yang masih harus dibuktikan ialah bahwa representasi tersebut tunggal. Sekarang misalkan

$$m = \sum_{i=0}^{l} a_i b^i = \sum_{i=0}^{s} c_i b^i.$$

Ambil $L = \max\{l, s\}$ dan tambahkan koefisien nol pada ekspansi yang lebih pendek. Dengan mengurangkan kedua ekspansi tersebut, diperoleh

$$\sum_{i=0}^{L} (a_i - c_i) b^i = 0.$$

Jika kedua ekspansi berbeda, ambil indeks terkecil $0 \leq j \leq L$ sedemikian sehingga $c_j \neq a_j$. Semua suku berindeks lebih kecil daripada j lenyap, sehingga diperoleh

$$b^j \sum_{i=j}^{L} (a_i - c_i) b^{i-j} = 0,$$

dan karena $b \neq 0$, diperoleh

$$\sum_{i=j}^{L} (a_i - c_i) b^{i-j} = 0.$$

Oleh karena itu,

$$a_j - c_j = -b \sum_{i=j+1}^{L} (a_i - c_i) b^{i-j-1},$$

sehingga $b \mid (a_j - c_j)$. Karena $0 \leq a_j < b$ dan $0 \leq c_j < b$, berlaku $|a_j - c_j| < b$. Dengan demikian, $a_j = c_j$. Ini bertentangan dengan pemilihan j, sehingga ekspansi tersebut tunggal. □

DEFINISI 1.4.2. Misalkan $b \in \mathbb{Z}$ memenuhi $b > 1$. Untuk $m \in \mathbb{N}$, misalkan $\ell \in \mathbb{Z}_{\geq 0}$ dan $a_0, a_1, \ldots, a_\ell \in \mathbb{Z}$ sebagaimana dalam teorema di atas (1.4.1). Maka **representasi basis** b **dari** m adalah rangkaian digit $(m)_b = a_\ell \ldots a_1 a_0$. Jika $b \geq 10$, kita sering menggunakan simbol tunggal lain untuk merepresentasikan nilai-nilai a_i yang mungkin, dari 10

sampai $b-1$. Sebagai contoh,

$$10 \leftrightsquigarrow A$$
$$11 \leftrightsquigarrow B$$
$$12 \leftrightsquigarrow C$$
$$\textit{dst.}$$

Representasi bilangan bulat dalam basis 2 disebut **representasi biner**. Representasi biner berguna bagi komputer: semua koefisien $a_0, \ldots, a_\ell$ dalam representasi biner memenuhi $0 \leq a_j < 2$, sehingga nilainya 0 atau 1. Jadi, untuk merepresentasikan bilangan bulat melalui $\ell + 1$ kawat, setiap kawat dapat diberi tegangan (1) atau tidak (0). (Istilah *bit* berasal dari frasa bahasa Inggris *binary digit*, yang berarti "digit biner".)

Pemrogram komputer juga sering menggunakan basis 8 dan basis 16, yang masing-masing disebut **oktal** dan **heksadesimal**, atau **heks**. Bangsa Babilonia menggunakan basis 60, yang disebut **seksagesimal**.

CONTOH 1.4.3. Untuk mencari ekspansi basis 3 dari 214, kita melakukan pembagian berikut:

$$\begin{aligned} 214 &= 3 \cdot 71 + 1 \\ 71 &= 3 \cdot 23 + 2 \\ 23 &= 3 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 3 \cdot 0 + 2 \end{aligned}$$

Untuk memperoleh ekspansi basis 3 dari 214, kita membaca sisa-sisa pembagian tersebut dari bawah ke atas, sehingga $(214)_{10} = (21221)_3$.

CONTOH 1.4.4. Untuk mencari ekspansi basis 10, yaitu ekspansi desimal, dari $(364)_7$, kita menghitung $4 \cdot 7^0 + 6 \cdot 7^1 + 3 \cdot 7^2 = 4 + 42 + 147 = 193$.

1.4.1. Latihan untuk §1.4.

LATIHAN 1.4.1. Ubah $(7482)_{10}$ ke notasi basis 6.

LATIHAN 1.4.2. Ubah $(98156)_{10}$ ke notasi basis 8.

LATIHAN 1.4.3. Ubah $(101011101)_2$ ke notasi desimal.

LATIHAN 1.4.4. Ubah $(AB6C7D)_{16}$ ke notasi desimal.

LATIHAN 1.4.5. Ubah $(9A0B)_{16}$ ke notasi biner.

1.5. Faktor Persekutuan Terbesar

Pada bagian ini kita mendefinisikan faktor persekutuan terbesar (FPB) dari dua bilangan bulat dan membahas sifat-sifatnya. Kita juga membuktikan bahwa FPB dua bilangan bulat merupakan kombinasi linear dari kedua bilangan tersebut.

Jika dua bilangan bulat a dan b tidak keduanya 0, setidaknya salah satunya taknol dan hanya mempunyai berhingga banyak pembagi (lihat Latihan 1.3.5). Karena itu, a dan b hanya mempunyai berhingga banyak pembagi bersama. Pada bagian ini kita membahas pembagi terbesar di antara pembagi-pembagi bersama tersebut.

DEFINISI 1.5.1. Untuk $a, b \in \mathbb{Z}$ yang tidak keduanya nol, **faktor persekutuan terbesar** adalah bilangan bulat terbesar yang membagi a sekaligus b, dan ditulis $\gcd(a, b)$ (atau kadang-kadang cukup (a, b)).

Jika hal ini menyederhanakan suatu rumus, kita menetapkan $\gcd(0, 0) = 0$.

CONTOH 1.5.2. Faktor persekutuan terbesar dari 24 dan 18 adalah 6. Dengan kata lain, $\gcd(24, 18) = 6$.

DEFINISI 1.5.3. Bilangan $a, b \in \mathbb{Z}$ disebut **relatif prima** jika $\gcd(a, b) = 1$.

CONTOH 1.5.4. Faktor persekutuan terbesar dari 9 dan 16 adalah 1; jadi, kedua bilangan tersebut relatif prima.

Perhatikan bahwa setiap bilangan bulat mempunyai pembagi positif dan negatif. Jika a adalah pembagi positif dari m, maka $-a$ juga merupakan pembagi dari m. Karena itu, dari definisi faktor persekutuan terbesar terlihat bahwa $\gcd(a, b) = \gcd(|a|, |b|)$.

Kita dapat menggunakan FPB dua bilangan bulat untuk membentuk bilangan-bilangan yang relatif prima:

TEOREMA 1.5.5. *Jika $a, b \in \mathbb{Z}$ tidak keduanya nol dan $\gcd(a, b) = d$, maka* $\gcd(a/d, b/d) = 1$.

BUKTI. Ambil $a, b \in \mathbb{Z}$. Kita akan menunjukkan bahwa a/d dan b/d tidak mempunyai pembagi bersama positif selain 1. Misalkan $k \in \mathbb{N}$ membagi a/d sekaligus b/d. Maka $\exists m, n \in \mathbb{Z}$ sedemikian sehingga

$$a/d = km \quad \text{dan} \quad b/d = kn$$

Dengan demikian,

$$a = kmd \quad \text{dan} \quad b = knd.$$

Jadi, kd merupakan pembagi bersama dari a dan b. Selain itu, $kd \geq d$. Namun, d adalah faktor persekutuan terbesar dari a dan b, sehingga $kd \leq d$. Oleh karena itu, $k = 1$. □

Teorema berikut menunjukkan bahwa faktor persekutuan terbesar dari dua bilangan bulat tidak berubah ketika suatu kelipatan dari salah satunya ditambahkan pada bilangan yang lain.

TEOREMA 1.5.6. *Misalkan* $a, b, c \in \mathbb{Z}$. *Maka* $\gcd(a, b) = \gcd(a + cb, b)$.

BUKTI. Kita akan menunjukkan bahwa setiap pembagi bersama dari a dan b juga merupakan pembagi bersama dari $a + cb$ dan b, demikian pula sebaliknya. Jadi, kedua pasangan itu mempunyai himpunan pembagi bersama yang persis sama. Karena itu, faktor persekutuan terbesar dari a dan b juga menjadi faktor persekutuan terbesar dari $a + cb$ dan b. Misalkan k adalah pembagi bersama dari a dan b. Menurut Teorema 1.3.9, $k \mid (a + cb)$, sehingga k membagi $a + cb$. Sekarang misalkan l adalah pembagi bersama dari $a + cb$ dan b. Sekali lagi, menurut Teorema 1.3.9,

$$l \mid ((a + cb) - cb) = a.$$

Jadi, l merupakan pembagi bersama dari a dan b, dan hasil yang dimaksud pun terbukti. □

CONTOH 1.5.7. Perhatikan bahwa $\gcd(4, 14) = \gcd(4, 14 - 3 \cdot 4) = \gcd(4, 2) = 2$.

Sekarang kita menyajikan teorema yang membuktikan bahwa faktor persekutuan terbesar dari dua bilangan bulat dapat ditulis sebagai kombinasi linear dari kedua bilangan tersebut.

TEOREMA 1.5.8. *Misalkan* $a, b \in \mathbb{Z}$ *tidak keduanya nol. Maka* $\gcd(a, b)$ *adalah bilangan asli terkecil yang berbentuk* $d = ma + nb$ *untuk suatu* $m, n \in \mathbb{Z}$.

BUKTI. Dengan mengganti a dan b masing-masing oleh $|a|$ dan $|b|$ serta menyerap tandanya ke dalam koefisien, tanpa mengurangi keumuman kita dapat menganggap $a, b \geq 0$ dan tidak keduanya nol. Tinjau himpunan

$$S = \{d \in \mathbb{N} \mid d = ma + nb \text{ untuk suatu } m, n \in \mathbb{Z}\}.$$

S tidak kosong karena setidaknya salah satu dari a dan b positif. Jika $a > 0$, maka $a = 1 \cdot a + 0 \cdot b \in S$; jika $b > 0$, maka $b = 0 \cdot a + 1 \cdot b \in S$. Misalkan $d \in \mathbb{N}$ adalah elemen terkecil dari S; keberadaannya dijamin oleh Prinsip Keterurutan Baik. Karena $d \in S$, terdapat $m, n \in \mathbb{Z}$ sedemikian sehingga $d = ma + nb$. Kita masih harus membuktikan bahwa d membagi a sekaligus b dan bahwa d adalah pembagi bersama terbesar dengan sifat tersebut.

Menurut Algoritma Pembagian, $\exists q, r \in \mathbb{Z}$ sedemikian sehingga

$$a = qd + r, \quad 0 \leq r < d.$$

Dengan demikian,

$$r = a - qd = a - q(ma + nb) = (1 - qm)a - qnb.$$

Jadi, r merupakan kombinasi linear dari a dan b. Karena $0 \leq r < d$ dan d adalah bilangan bulat positif terkecil yang merupakan kombinasi linear dari a dan b, haruslah $r = 0$, sehingga $a = qd$. Jadi, $d \mid a$.

Argumen yang sama menunjukkan bahwa $d \mid b$.

Sekarang, misalkan c membagi a sekaligus b. Menurut Teorema 1.3.9, c membagi setiap kombinasi linear dari a dan b. Jadi, $c \mid d$. Hal ini membuktikan bahwa setiap pembagi bersama dari a dan b membagi d. Karena itu, $c \leq d$, dan d adalah faktor persekutuan terbesar. □

Berikut suatu penerapan sederhana yang akan sangat berguna kelak:

AKIBAT 1.5.9. *Jika $a, b \in \mathbb{Z}$ relatif prima, maka $\exists m, n \in \mathbb{Z}$ sedemikian sehingga $ma + nb = 1$.*

DEFINISI 1.5.10. Untuk suatu $n \in \mathbb{N}$, misalkan $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tidak semuanya 0. **Faktor persekutuan terbesar** dari bilangan-bilangan tersebut adalah bilangan bulat terbesar yang membagi semuanya, dan dilambangkan dengan $\gcd(a_1, \ldots, a_n)$.

DEFINISI 1.5.11. Untuk suatu $n \in \mathbb{N}$, bilangan-bilangan $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ disebut **relatif prima secara bersama-sama** jika $\gcd(a_1, a_2, \ldots, a_n) = 1$.

CONTOH 1.5.12. Bilangan-bilangan bulat $3, 6, 7$ relatif prima secara bersama-sama karena $(3, 6, 7) = 1$, meskipun $(3, 6) = 3$.

DEFINISI 1.5.13. Untuk suatu $n \in \mathbb{N}$, bilangan-bilangan $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ disebut **relatif prima berpasangan** jika $\forall i, j \in \mathbb{N}$ dengan $i \leq n$, $j \leq n$, dan $i \neq j$, berlaku $\gcd(a_i, a_j) = 1$.

CONTOH 1.5.14. Bilangan-bilangan bulat $3, 14, 25$ relatif prima berpasangan. Perhatikan pula bahwa bilangan-bilangan tersebut relatif prima secara bersama-sama.

PROPOSISI 1.5.15. *Untuk $n \in \mathbb{N}$ dengan $n \geq 2$ dan $a_1, \ldots, a_n \in \mathbb{Z}$, jika $a_1, a_2, \ldots, a_n$ relatif prima berpasangan, maka bilangan-bilangan tersebut relatif prima secara bersama-sama.*

Latihan untuk §1.5.

LATIHAN 1.5.1. Tentukan faktor persekutuan terbesar dari 15 dan 35.

LATIHAN 1.5.2. Tentukan faktor persekutuan terbesar dari 100 dan 104.

LATIHAN 1.5.3. Tentukan faktor persekutuan terbesar dari -30 dan 95.

LATIHAN 1.5.4. Misalkan $m \in \mathbb{N}$. Tentukan faktor persekutuan terbesar dari m dan $m+1$.

LATIHAN 1.5.5. Misalkan $m \in \mathbb{N}$. Tentukan faktor persekutuan terbesar dari m dan $m+2$.

LATIHAN 1.5.6. Tunjukkan bahwa jika $m, n \in \mathbb{Z}$ memenuhi $\gcd(m,n) = 1$, maka $\gcd(m+n, m-n) = 1$ atau 2.

LATIHAN 1.5.7. Tunjukkan bahwa jika $m \in \mathbb{N}$, maka $3m+2$ dan $5m+3$ relatif prima.

LATIHAN 1.5.8. Tunjukkan bahwa jika $a, b \in \mathbb{Z}$ relatif prima, maka $\gcd(a+2b, 2a+b) = 1$ atau 3.

LATIHAN 1.5.9. Tunjukkan bahwa jika $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tidak semuanya 0 dan $c \in \mathbb{N}$, maka $\gcd(ca_1, ca_2, \ldots, ca_n) = c \cdot \gcd(a_1, a_2, \ldots, a_n)$.

1.6. Algoritma Euklides

Pada bagian ini kita menjelaskan metode sistematis untuk menentukan faktor persekutuan terbesar dari dua bilangan bulat. Metode ini berasal dari Euklides dan karena itu disebut Algoritma Euklides.

LEMA 1.6.1. *Jika* $a, b, q, r \in \mathbb{Z}$ *dan* $a = qb + r$*, maka* $\gcd(a, b) = \gcd(r, b)$.

BUKTI. Menurut sifat invariansi FPB terhadap penambahan kelipatan yang dibuktikan pada bagian sebelumnya, $\gcd(bq + r, b) = \gcd(b, r)$. □

Sekarang kita beralih ke bentuk umum Algoritma Euklides. Pada dasarnya, algoritma ini menyatakan bahwa faktor persekutuan terbesar dari dua bilangan bulat adalah sisa taknol terakhir dalam pembagian berulang.

TEOREMA 1.6.2. *Misalkan* $a, b \in \mathbb{N}$ *dan* $a \geq b$*. Tetapkan* $r_0 = a$*,* $r_1 = b$*,* $s_0 = 1$*,* $s_1 = 0$*,* $t_0 = 0$*, dan* $t_1 = 1$*. Terapkan Algoritma Pembagian secara berulang: selama* $r_{j+1} \neq 0$*, tentukan* $q_{j+1} \in \mathbb{N}$ *dan* $r_{j+2} \in \mathbb{Z}_{\geq 0}$ *sedemikian sehingga* $r_j = r_{j+1}q_{j+1} + r_{j+2}$ *dan* $0 \leq r_{j+2} < r_{j+1}$*. Berhentilah pada indeks* n *yang memenuhi* $r_n > 0$ *dan* $r_{n+1} = 0$*. Pada setiap langkah, tetapkan* $s_{j+2} = s_j - q_{j+1}s_{j+1}$ *dan* $t_{j+2} = t_j - q_{j+1}t_{j+1}$*. Maka* $\gcd(a, b) = r_n = s_n a + t_n b$.

BUKTI. Dengan menerapkan Algoritma Pembagian, diperoleh

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, \qquad 0 \leq r_{j+2} < r_{j+1} \quad (j = 0, 1, \ldots, n-1).$$

Proses ini akhirnya menghasilkan sisa 0, sebab selama sisanya taknol, sisa-sisa tersebut membentuk barisan menurun ketat dari bilangan bulat taknegatif. Menurut Lema 1.6.1,

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n.$$

□

Catatan: Versi lengkap teorema ini, yang menyertakan s_j dan t_j, disebut **Algoritma Euklides diperluas**, sedangkan versi yang lebih sederhana tanpa koefisien-koefisien tersebut disebut **Algoritma Euklides**.

Pembaca yang teliti akan melihat bahwa kita belum membuktikan klaim bahwa s_j dan t_j dapat digunakan untuk menuliskan FPB sebagai kombinasi linear dari a dan b. Bukti tersebut diserahkan sebagai latihan di bawah ini.

CONTOH 1.6.3. Kita akan menentukan faktor persekutuan terbesar dari 4147 dan 10672. Perhatikan bahwa

$$\begin{aligned} 10672 &= 4147 \cdot 2 + 2378, \\ 4147 &= 2378 \cdot 1 + 1769, \\ 2378 &= 1769 \cdot 1 + 609, \\ 1769 &= 609 \cdot 2 + 551, \\ 609 &= 551 \cdot 1 + 58, \\ 551 &= 58 \cdot 9 + 29, \\ 58 &= 29 \cdot 2, \end{aligned}$$

Jadi, $\gcd(4147, 10672) = 29$.

Latihan untuk §1.6.

LATIHAN 1.6.1. Gunakan Algoritma Euklides untuk menentukan faktor persekutuan terbesar dari 412 dan 32, lalu nyatakan hasilnya sebagai kombinasi linear kedua bilangan tersebut.

LATIHAN 1.6.2. Gunakan Algoritma Euklides untuk menentukan faktor persekutuan terbesar dari 780 dan 150, lalu nyatakan hasilnya sebagai kombinasi linear kedua bilangan tersebut.

LATIHAN 1.6.3. Tentukan faktor persekutuan terbesar dari $70, 98, 108$.

LATIHAN 1.6.4. Misalkan $a, b \in \mathbb{N}$ genap. Buktikan bahwa $\gcd(a, b) = 2\gcd(a/2, b/2)$.

LATIHAN 1.6.5. Tunjukkan bahwa jika $a \in \mathbb{N}$ genap dan $b \in \mathbb{N}$ ganjil, maka $\gcd(a, b) = \gcd(a/2, b)$.

LATIHAN 1.6.6. Buktikan klaim mengenai koefisien dalam Algoritma Euklides diperluas.

BAB 2

Kongruensi

Kongruensi tidak lebih dari sebuah pernyataan mengenai keterbagian. Teori kongruensi diperkenalkan oleh Carl Friedrich Gauss, dalam karya monumentalnya *Disquisitiones Arithmeticae* (diterbitkan pada tahun 1801, ketika ia berusia 24 tahun; terjemahannya terdapat dalam [**Gau86**]).

Kita mulai dengan memperkenalkan kongruensi beserta sifat-sifatnya. Kemudian kita menyajikan solusi kongruensi linear sebagai pengantar menuju Teorema Sisa Cina yang akan dibahas sesudahnya.

2.1. Pengantar Kongruensi

Seperti disebutkan dalam pengantar, teori kongruensi dikembangkan oleh Gauss pada awal abad kesembilan belas.

DEFINISI 2.1.1. Untuk $a, b \in \mathbb{Z}$ dan $n \in \mathbb{N}$, kita mengatakan bahwa a **kongruen dengan** b **modulo** n jika $n \mid (a - b)$, yakni jika $\exists k \in \mathbb{Z}$ sedemikian sehingga $a = b + kn$. Jika a kongruen dengan b modulo n, kita menulis $a \equiv b \pmod{n}$.

CONTOH 2.1.2. $19 \equiv 5 \pmod{7}$. Demikian pula, $2k + 1 \equiv 1 \pmod{2}$, yang berarti bahwa setiap bilangan ganjil kongruen dengan 1 modulo 2.

Dalam banyak hal, kongruensi sangat menyerupai kesamaan. Sebagai contoh:

TEOREMA 2.1.3. *Misalkan* $a, b, c, d \in \mathbb{Z}$ *dan* $n \in \mathbb{N}$. *Maka*

(1) *Jika* $a \equiv b \pmod{n}$, *maka* $b \equiv a \pmod{n}$.
(2) *Jika* $a \equiv b \pmod{n}$ *dan* $b \equiv c \pmod{n}$, *maka* $a \equiv c \pmod{n}$.
(3) *Jika* $a \equiv b \pmod{n}$, *maka* $a + c \equiv b + c \pmod{n}$.
(4) *Jika* $a \equiv b \pmod{n}$, *maka* $a - c \equiv b - c \pmod{n}$.
(5) *Jika* $a \equiv b \pmod{n}$, *maka* $ac \equiv bc \pmod{n}$.
(6) *Jika* $c > 0$ *dan* $a \equiv b \pmod{n}$, *maka* $ac \equiv bc \pmod{nc}$.
(7) *Jika* $a \equiv b \pmod{n}$ *dan* $c \equiv d \pmod{n}$, *maka* $a + c \equiv b + d \pmod{n}$.
(8) *Jika* $a \equiv b \pmod{n}$ *dan* $c \equiv d \pmod{n}$, *maka* $a - c \equiv b - d \pmod{n}$.
(9) *Jika* $a \equiv b \pmod{n}$ *dan* $c \equiv d \pmod{n}$, *maka* $ac \equiv bd \pmod{n}$.

BUKTI.

(1) Jika $a \equiv b \pmod{n}$, maka $n \mid (a-b)$. Jadi terdapat $k \in \mathbb{Z}$ sedemikian sehingga $a - b = kn$. Hal ini mengakibatkan $b - a = (-k)n$, sehingga $n \mid (b-a)$. Dengan demikian, $b \equiv a \pmod{n}$.

(2) Karena $a \equiv b \pmod{n}$ dan $b \equiv c \pmod{n}$, berlaku $n \mid (a-b)$ dan $n \mid (b-c)$. Oleh karena itu, terdapat $k, l \in \mathbb{Z}$ sedemikian sehingga $a = b + kn$ dan $b = c + ln$. Akibatnya, $a = c + (k+l)n$. Dengan kata lain, $a \equiv c \pmod{n}$.

(3) Karena $a \equiv b \pmod{n}$, berlaku $n \mid (a-b)$. Dengan menambahkan dan mengurangkan c, kita memperoleh

$$n \mid ((a+c) - (b+c))$$

yang berarti bahwa

$$a + c \equiv b + c \pmod{n}.$$

(4) Karena $a \equiv b \pmod{n}$, berlaku $n \mid (a-b)$. Dengan mengurangkan dan menambahkan c, kita memperoleh

$$n \mid ((a-c) - (b-c))$$

sehingga

$$a - c \equiv b - c \pmod{n}.$$

(5) Jika $a \equiv b \pmod{n}$, maka $n \mid (a-b)$. Jadi terdapat $k \in \mathbb{Z}$ sedemikian sehingga $a - b = kn$, dan akibatnya $ac - bc = (kc)n$. Oleh karena itu,

$$n \mid (ac - bc)$$

dan dengan demikian

$$ac \equiv bc \pmod{n}.$$

(6) Jika $a \equiv b \pmod{n}$, maka $n \mid (a-b)$. Jadi terdapat $k \in \mathbb{Z}$ sedemikian sehingga $a - b = kn$, dan akibatnya

$$ac - bc = kcn.$$

Jadi,

$$nc \mid (ac - bc)$$

dan dengan demikian

$$ac \equiv bc \pmod{nc}.$$

(7) Karena $a \equiv b \pmod{n}$ dan $c \equiv d \pmod{n}$, berlaku $n \mid (a-b)$ dan $n \mid (c-d)$. Oleh karena itu, terdapat $k, l \in \mathbb{Z}$ sedemikian sehingga $a - b = kn$ dan $c - d = ln$. Perhatikan bahwa

$$(a-b) + (c-d) = (a+c) - (b+d) = (k+l)n.$$

Akibatnya,

$$n \mid ((a+c)-(b+d)),$$

sehingga

$$a+c \equiv b+d \pmod{n}.$$

(8) Jika $a = b+kn$ dan $c = d+ln$ untuk $k, l \in \mathbb{Z}$, maka

$$(a-b)-(c-d) = (a-c)-(b-d) = (k-l)n.$$

Akibatnya,

$$n \mid ((a-c)-(b-d)),$$

sehingga

$$a-c \equiv b-d \pmod{n}.$$

(9) Terdapat $k, l \in \mathbb{Z}$ sedemikian sehingga $a-b = kn$ dan $c-d = ln$. Dengan demikian, $ca-cb = (ck)n$ dan $bc-bd = (bl)n$. Perhatikan bahwa

$$(ca-cb)+(bc-bd) = ac-bd = (ck+bl)n.$$

Akibatnya,

$$n \mid (ac-bd),$$

sehingga

$$ac \equiv bd \pmod{n}.$$

□

Berikut sebuah hasil teknis yang akan berguna kelak:

TEOREMA 2.1.4. *Misalkan $a, b, c \in \mathbb{Z}$. Jika $a \mid c$, $b \mid c$, serta a dan b relatif prima, maka $ab \mid c$.*

BUKTI. Berdasarkan Akibat 1.5.9, terdapat $m, n \in \mathbb{Z}$ sedemikian sehingga $ma+nb = 1$. Dari hipotesis keterbagian, terdapat pula $p, q \in \mathbb{Z}$ sedemikian sehingga $c = pa$ dan $c = qb$. Kita hitung:

$$c = c \cdot 1 = c(ma+nb) = mca + ncb = mqba + npab = (mq+np)ab\ .$$

Ini berarti $ab \mid c$, seperti yang diinginkan. □

CONTOH-CONTOH 2.1.5.

(1) $14 \equiv 8 \pmod{6}$, *sehingga* $8 \equiv 14 \pmod{6}$.
(2) *Karena* $22 \equiv 10 \pmod{6}$ *dan* $10 \equiv 4 \pmod{6}$, *berlaku pula* $22 \equiv 4 \pmod{6}$.
(3) $50 \equiv 20 \pmod{15}$, *sehingga* $50+5 = 55 \equiv 20+5 = 25 \pmod{15}$.
(4) $50 \equiv 20 \pmod{15}$, *sehingga* $50-5 = 45 \equiv 20-5 = 15 \pmod{15}$.
(5) $19 \equiv 16 \pmod{3}$, *sehingga* $2(19) = 38 \equiv 2(16) = 32 \pmod{3}$.
(6) $19 \equiv 16 \pmod{3}$, *sehingga* $2(19) = 38 \equiv 2(16) = 32 \pmod{2 \cdot 3}$, *atau* $38 \equiv 2(16) = 32 \pmod{6}$.

(7) *Karena* $19 \equiv 3 \pmod 8$ *dan* $17 \equiv 9 \pmod 8$*, kita memperoleh* $19 + 17 = 36 \equiv 3 + 9 = 12 \pmod 8$.
(8) *Karena* $19 \equiv 3 \pmod 8$ *dan* $17 \equiv 9 \pmod 8$*, kita memperoleh* $19 - 17 = 2 \equiv 3 - 9 = -6 \pmod 8$.
(9) *Karena* $19 \equiv 3 \pmod 8$ *dan* $17 \equiv 9 \pmod 8$*, kita memperoleh* $19(17) = 323 \equiv 3(9) = 27 \pmod 8$.

Berikut sebuah hasil yang pada awalnya tampak sangat sederhana, tetapi ternyata amat berguna — sedemikian bergunanya sehingga hasil ini memiliki nama.

LEMA 2.1.6. **Lemma Euklides:** *Misalkan* $x, y, z \in \mathbb{Z}$*. Jika* $x \mid yz$ *dan* $\gcd(x, y) = 1$*, maka* $x \mid z$.

BUKTI. Dari Akibat 1.5.9, terdapat $m, n \in \mathbb{Z}$ sedemikian sehingga $mx + ny = 1$. Dengan mengalikan kedua ruas dengan z, kita memperoleh $mxz + nyz = z$. Namun, berdasarkan asumsi $x \mid yz$, berlaku $x \mid nyz$; jelas pula bahwa $x \mid mxz$. Jadi $x \mid mxz+nyz$, yakni $x \mid z$. □

Sekarang kita menyajikan sebuah teorema yang memperlihatkan salah satu perbedaan antara persamaan dan kongruensi. Pada persamaan, kesamaan tetap berlaku jika kedua ruas dibagi dengan suatu bilangan tak nol. Namun, pada kongruensi, hal ini belum tentu berlaku. Dengan kata lain, membagi kedua ruas suatu kongruensi dengan bilangan bulat yang sama belum tentu mempertahankan kongruensi tersebut.

TEOREMA 2.1.7.

(1) *Misalkan* $a, b, c \in \mathbb{Z}$ *dan* $n \in \mathbb{N}$*, serta definisikan* $d = \gcd(a, n) \in \mathbb{N}$*. Jika* $ab \equiv ac \pmod n$*, maka* $b \equiv c \pmod{n/d}$.
(2) *Secara khusus, jika* $\gcd(a, n) = 1$*, maka*

$$b \equiv c \pmod n \qquad \Leftrightarrow \qquad ab \equiv ac \pmod n.$$

BUKTI. Untuk Bagian 1, jika $ab \equiv ac \pmod n$, maka

$$n \mid (ab - ac) = a(b - c).$$

Jadi terdapat $k \in \mathbb{Z}$ sedemikian sehingga $a(b - c) = kn$. Dengan membagi kedua ruas dengan d, kita memperoleh $(a/d)(b-c) = k(n/d)$, atau $(n/d) \mid (a/d)(b-c)$. Berdasarkan Teorema 1.5.5, $\gcd(a/d, n/d) = 1$. Karena itu, Lemma Euklides 2.1.6 menyatakan bahwa $(n/d) \mid (b - c)$. Dengan demikian, $b \equiv c \pmod{n/d}$.

Untuk Bagian 2, arah $\Rightarrow$ merupakan Bagian 5 dari Teorema 2.1.3, sedangkan arah $\Leftarrow$ merupakan kasus khusus dari Bagian 1. □

CONTOH 2.1.8. $38 \equiv 10 \pmod 7$. Karena $\gcd(2, 7) = 1$, kita memperoleh $19 \equiv 5 \pmod 7$.

Pada tahap ini, satu hasil teknis terakhir patut dinyatakan dengan jelas:

TEOREMA 2.1.9. *Misalkan $n, d \in \mathbb{N}$ dengan $d \mid n$. Terdapat tepat d kelas solusi $x \in \mathbb{Z}$ modulo n yang memenuhi $x \equiv 0 \pmod{n/d}$.*

BUKTI. Misalkan $x_j = j(n/d)$ untuk $j = 0, \ldots, (d-1)$. Jelas bahwa masing-masing dari d nilai x_j ini merupakan kelipatan n/d, sehingga memenuhi $x \equiv 0 \pmod{n/d}$. Jadi, kita hanya perlu menunjukkan bahwa *setiap* solusi x dari $x \equiv 0 \pmod{n/d}$ kongruen modulo n dengan salah satu x_j tersebut.

Misalkan x adalah solusi semacam itu. Maka terdapat $k \in \mathbb{Z}$ sedemikian sehingga $x = k(n/d)$. Terapkan Algoritma Pembagian untuk membagi x dengan n, sehingga $x = qn + r$ untuk suatu $q, r \in \mathbb{Z}$ dengan $0 \leq r < n$. Namun,

$$r = x - qn = k(n/d) - qd(n/d) = (k - qd)(n/d)$$

sehingga r merupakan kelipatan (n/d) yang terletak dalam rentang $[0, n)$. Kelipatan-kelipatan semacam itu hanyalah $x_0, \ldots, x_{(d-1)}$ yang didefinisikan di atas; misalkan $r = x_j$. Maka $x = qn + r = qn + x_j \equiv x_j \pmod{n}$. Dengan demikian, setiap solusi x kongruen modulo n dengan tepat satu dari d solusi khusus $x_0, \ldots, x_{(d-1)}$. □

Latihan untuk §2.1.

LATIHAN 2.1.1. Tentukan apakah 3 dan 99 kongruen modulo 7.

LATIHAN 2.1.2. Buktikan bahwa jika x adalah bilangan bulat ganjil, maka $x^2 \equiv 1 \pmod 8$.

LATIHAN 2.1.3. Buktikan bahwa jika $a, b \in \mathbb{Z}$ dan $m, n \in \mathbb{N}$ memenuhi $n \mid m$ dan $a \equiv b \pmod m$, maka $a \equiv b \pmod n$.

LATIHAN 2.1.4. Buktikan bahwa jika $n, k \in \mathbb{N}$ dan $\{a_1, \ldots, a_k, b_1, \ldots, b_k\} \subset \mathbb{Z}$ memenuhi $a_i \equiv b_i \pmod n$ untuk $i = 1, 2, \ldots, k$, maka $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod n$.

LATIHAN 2.1.5. Untuk nilai $n \in \mathbb{N}$ manakah berlaku $1 + 2 + \cdots + (n-1) \equiv 0 \pmod n$?

2.2. Kongruensi Linear

Karena kongruensi beranalogi dengan kesamaan, wajar jika kita menanyakan padanan persamaan linear — persamaan paling sederhana yang dapat diselesaikan dalam aljabar — dengan menggunakan kongruensi sebagai pengganti kesamaan. Dalam bagian ini, kita membahas kongruensi linear dalam satu peubah beserta solusi-solusinya.

Kita mulai dengan sebuah definisi:

DEFINISI 2.2.1. Untuk konstanta $a, b \in \mathbb{Z}$ dan $n \in \mathbb{N}$, kongruensi berbentuk $ax \equiv b \pmod{n}$, dengan $x \in \mathbb{Z}$ sebagai peubah yang tidak diketahui, disebut **kongruensi linear dalam satu peubah**.

Jika suatu kongruensi linear memiliki satu solusi, maka kongruensi itu memiliki tak terhingga banyak solusi:

TEOREMA 2.2.2. *Misalkan $a, b \in \mathbb{Z}$ dan $n \in \mathbb{N}$ adalah konstanta, serta $x \in \mathbb{Z}$ merupakan solusi kongruensi linear $ax \equiv b \pmod{n}$. Setiap $x' \in \mathbb{Z}$ lain yang memenuhi $x' \equiv x \pmod{n}$ juga merupakan solusi kongruensi yang sama.*

[Catatan: pada masa awal perkembangan teori bilangan, sebelum Gauss, kongruensi linear dibahas melalui persamaan Diofantin berikut.

DEFINISI 2.2.3. Persamaan polinomial dengan koefisien bilangan bulat yang solusi-solusinya dicari dalam bilangan bulat disebut **persamaan Diofantin**.

Dalam istilah ini, kongruensi linear modern $ax \equiv b \pmod{n}$, untuk $a, b \in \mathbb{Z}$ dan $n \in \mathbb{N}$, setara dengan persamaan Diofantin linear $ax - ny = b$ dalam dua peubah tak diketahui, x dan y.]

Hasil berikut memberikan karakterisasi yang cukup lengkap bagi solusi kongruensi linear:

TEOREMA 2.2.4. *Misalkan $a, b \in \mathbb{Z}$ dan $n \in \mathbb{N}$, dan tinjau kongruensi linear*

$$ax \equiv b \pmod{n}.$$

Dengan menetapkan $d = \gcd(a, n)$, berlaku

(1) *Jika $d \nmid b$, maka kongruensi tersebut tidak memiliki solusi.*
(2) *Jika $d \mid b$, maka kongruensi tersebut memiliki tepat d solusi yang berbeda modulo n.*

BUKTI. Untuk Bagian 1, kita membuktikan kontraposisinya. Andaikan kongruensi tersebut memiliki solusi. Artinya, terdapat $x, k \in \mathbb{Z}$ sedemikian sehingga $ax - b = kn$, atau $ax - kn = b$. Karena $d = \gcd(a, n)$ merupakan pembagi bersama a dan n, bilangan d membagi kombinasi linear $ax - kn = b$. Jadi $d \mid b$.

Untuk Bagian 2, andaikan $d \mid b$, sehingga terdapat $k \in \mathbb{Z}$ sedemikian sehingga $kd = b$. Dari Teorema 1.5.8, terdapat $p, q \in \mathbb{Z}$ sedemikian sehingga $d = pa + qn$. Ini berarti $kpa + kqn = kd = b$, atau setelah disusun ulang, $a(kp) - b = (-kq)n$. Jadi $n \mid (a(kp) - b)$, yakni $a(kp) \equiv b \pmod{n}$. Dengan demikian, $x = kp$ merupakan salah satu solusi kongruensi linear $ax \equiv b \pmod{n}$.

Terakhir, mari kita buktikan banyaknya solusi modulo n. Kita baru saja melihat bahwa terdapat setidaknya satu $x \in \mathbb{Z}$ yang memenuhi $ax \equiv b \pmod{n}$. Misalkan $y \in \mathbb{Z}$ adalah solusi lain. Maka $ax \equiv b \equiv ay \pmod{n}$. Berdasarkan Bagian 1 dari Teorema 2.1.7, berlaku $x \equiv y \pmod{n/d}$, atau $\delta = y - x \equiv 0 \pmod{n/d}$. Menurut Teorema 2.1.9, terdapat tepat d kemungkinan untuk δ modulo n. Karena itu, terdapat paling banyak d kelas solusi.

Sebaliknya, ambil salah satu dari d kelas δ modulo n yang memenuhi $\delta \equiv 0 \pmod{n/d}$, lalu pilih sebuah wakil yang juga kita namai δ. Terdapat $t \in \mathbb{Z}$ sedemikian sehingga $\delta = t(n/d)$. Karena $d \mid a$, terdapat $a' \in \mathbb{Z}$ dengan $a = da'$, sehingga $a\delta = a'tn$ dan $n \mid a\delta$. Oleh sebab itu, $a(x + \delta) \equiv ax \equiv b \pmod{n}$. Penambahan oleh x mempertahankan perbedaan kelas modulo n, sehingga setiap kelas δ tersebut menghasilkan kelas solusi yang berbeda. Jadi kongruensi ini memiliki tepat d solusi yang berbeda modulo n. □

CATATAN 2.2.5. Perhatikan bahwa jika $a \in \mathbb{Z}$ dan $n \in \mathbb{N}$ relatif prima, maka untuk setiap $b \in \mathbb{Z}$ terdapat tepat satu solusi modulo n bagi kongruensi $ax \equiv b \pmod{n}$.

CONTOH 2.2.6. Mari kita cari semua solusi kongruensi $3x \equiv 12 \pmod{6}$. Perhatikan bahwa $\gcd(3, 6) = 3$ dan $3 \mid 12$. Jadi terdapat tiga solusi yang tidak kongruen satu sama lain modulo 6. Dengan menggunakan Algoritma Euklides untuk mencari solusi persamaan $3x - 6y = 12$, kita memperoleh solusi $x_0 = 6$. Dengan demikian, ketiga kelas solusi modulo 6 diberikan oleh $x_0 \equiv 6 \equiv 0 \pmod{6}$, $x_1 \equiv 6 + 2 \equiv 2 \pmod{6}$, dan $x_2 \equiv 6 + 4 \equiv 4 \pmod{6}$.

Seperti disebutkan dalam Catatan 2.2.5, kongruensi $ax \equiv b \pmod{n}$ untuk $a, b \in \mathbb{Z}$ dan $n \in \mathbb{N}$ memiliki solusi tunggal modulo n jika $\gcd(a, n) = 1$. Hal ini memungkinkan kita membahas *invers modular*.

DEFINISI 2.2.7. Misalkan $a \in \mathbb{Z}$ dan $n \in \mathbb{N}$ dengan $\gcd(a, n) = 1$. Suatu solusi kongruensi $ax \equiv 1 \pmod{n}$ disebut **invers** a **modulo** n. Kita menyatakan invers semacam itu dengan a^{-1}; nilai n dipahami dari konteks.

Dengan menyatakan secara formal hal yang baru saja diingatkan oleh Catatan 2.2.5, kita memperoleh

AKIBAT 2.2.8. *Jika $a \in \mathbb{Z}$ dan $n \in \mathbb{N}$ relatif prima, maka invers modular a^{-1} ada dan tunggal modulo n.*

CONTOH 2.2.9. Invers modular 7^{-1} dari 7 modulo 48 adalah 7. Perhatikan bahwa salah satu solusi $7x \equiv 1 \pmod{48}$ ialah $x \equiv 7 \pmod{48}$.

Latihan untuk §2.2.

LATIHAN 2.2.1. Carilah semua solusi $3x \equiv 6 \pmod 9$.

LATIHAN 2.2.2. Carilah semua solusi $3x \equiv 2 \pmod 7$.

LATIHAN 2.2.3. Carilah invers 2 dan 11 modulo 13.

LATIHAN 2.2.4. Misalkan $a, b \in \mathbb{Z}$ dan $n \in \mathbb{N}$. Buktikan bahwa jika a^{-1} adalah invers a modulo n dan b^{-1} adalah invers b modulo n, maka $a^{-1}b^{-1}$ adalah invers ab modulo n.

2.3. Teorema Sisa Cina

Dalam bagian ini, kita membahas solusi sistem kongruensi dengan modulus yang berbeda-beda. Salah satu contoh sistem semacam itu adalah sebagai berikut: carilah bilangan yang menyisakan 1 ketika dibagi 2, menyisakan 2 ketika dibagi 3, dan menyisakan 3 ketika dibagi 5. Kita akan melihat bahwa terdapat cara sistematis untuk menyelesaikan sistem semacam ini.

TEOREMA 2.3.1. ***Teorema Sisa Cina:*** *Tetapkan $k \in \mathbb{N}$. Untuk $b_1, \ldots, b_k \in \mathbb{Z}$ dan $n_1, \ldots, n_k \in \mathbb{N}$, sistem kongruensi*

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

memiliki solusi $x \in \mathbb{Z}$ jika $n_1, n_2, \ldots, n_k$ relatif prima berpasangan. Solusinya tunggal modulo $N = n_1\, n_2 \ldots n_k$.

BUKTI. Untuk $j = 1, \ldots, k$, misalkan $N_j = N/n_j$. Karena modulus-modulus n_j relatif prima berpasangan, $\gcd(N_j, n_j) = 1$ — sebab N_j merupakan hasil kali semua modulus selain n_j. Berdasarkan Akibat 2.2.8, terdapat invers $y_j = N_j^{-1}$ modulo n_j yang memenuhi $N_j y_j \equiv 1 \pmod{n_j}$. Sekarang, tinjau

$$x = \sum_{j=1}^{k} b_j N_j y_j$$

Karena

$$N_j \equiv 0 \pmod{n_i} \ \forall i \neq j,$$

kita memperoleh

$$x \equiv b_j N_j y_j \equiv b_j \pmod{n_j}.$$

Jadi, x merupakan solusi sistem kongruensi tersebut.

Sekarang kita perlu menunjukkan bahwa setiap dua solusi kongruen modulo N. Misalkan x dan y keduanya merupakan solusi sistem kongruensi tersebut. Maka $x \equiv b_j \equiv y \pmod{n_j}$, atau $n_j \mid x - y$, untuk setiap $1 \leq j \leq k$. Karena modulus-modulus itu relatif prima berpasangan, dengan menerapkan Teorema 2.1.4 berulang kali (secara formal, melalui induksi), kita menyimpulkan bahwa $N = n_1 \ldots n_k \mid x - y$, atau $x \equiv y \pmod{N}$. □

CONTOH 2.3.2. Selesaikan sistem

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5.$$

Kita memperoleh $N = 2 \cdot 3 \cdot 5 = 30$. Selain itu,

$$N_1 = 30/2 = 15,\ N_2 = 30/3 = 10,\ \text{dan}\ N_3 = 30/5 = 6.$$

Sekarang kita perlu menyelesaikan $15y_1 \equiv 1 \pmod 2$; salah satu solusinya adalah $y_1 \equiv 1 \pmod 2$. Dengan cara yang sama, kita memperoleh $y_2 \equiv 1 \pmod 3$ dan $y_3 \equiv 1 \pmod 5$. Oleh karena itu,

$$x = 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 = 53 \equiv 23 \pmod{30}.$$

Latihan untuk §2.3.

LATIHAN 2.3.1. Carilah bilangan bulat yang menyisakan 2 ketika dibagi 3 maupun 5, tetapi habis dibagi 4.

LATIHAN 2.3.2. Carilah semua bilangan bulat yang menyisakan 4 ketika dibagi 11 dan menyisakan 3 ketika dibagi 17.

LATIHAN 2.3.3. Carilah semua bilangan bulat yang menyisakan 1 ketika dibagi 2, menyisakan 2 ketika dibagi 3, dan menyisakan 3 ketika dibagi 5.

LATIHAN 2.3.4. Sekelompok 17 bajak laut mencuri sejumlah batangan emas. Ketika mereka mencoba membagi hasil rampasan itu secara merata, tersisa 3 batang; perkelahian pun pecah dan menewaskan satu orang. Mereka segera tenang dan memeriksa apakah emas itu kini dapat dibagi rata. Sayangnya, masih tersisa 10 batang, sehingga mereka bertarung lagi. Setelah satu korban jiwa lagi yang tak terelakkan, emas itu akhirnya dapat dibagi rata tanpa sisa. Berapakah jumlah minimum batangan emas yang mungkin mereka miliki pada awalnya? *[Soal ini tampaknya merupakan soal Cina kuno.]*

2.4. Cara Lain Menangani Kongruensi: Kelas Ekuivalensi

Dalam bagian ini, kita akan mempelajari cara lain untuk menangani kongruensi, berdasarkan gagasan berikut.

DEFINISI 2.4.1. Misalkan S suatu himpunan dan $\cong$ suatu *relasi* yang didefinisikan pada S. (Artinya, untuk setiap $x, y \in S$, pernyataan "$x \cong y$" dapat bernilai benar atau salah.) Jika $\cong$ memenuhi ketiga sifat berikut, relasi itu disebut **relasi ekuivalensi**:

- *[Refleksivitas]* $\forall x \in S$, $x \cong x$.
- *[Simetri]* $\forall x, y \in S$, $x \cong y \Leftrightarrow y \cong x$.
- *[Transitivitas]* $\forall x, y, z \in S$, $x \cong y$ dan $y \cong z \Rightarrow x \cong z$.

Jika $\cong$ merupakan relasi ekuivalensi pada himpunan S dan $x \in S$, maka himpunan $[x] = \{y \in S \mid y \cong x\} \subseteq S$ disebut **kelas ekuivalensi dari** x. Kita menulis $S/\cong$ untuk himpunan semua kelas ekuivalensi dalam S. Jika $\mathcal{C} \in S/\cong$, maka setiap $r \in S$ yang memenuhi $\mathcal{C} = [r]$ disebut **wakil kelas ekuivalensi** $\mathcal{C}$.

TEOREMA 2.4.2. *Misalkan S suatu himpunan dan $\cong$ suatu relasi ekuivalensi yang didefinisikan pada S. Maka*

(1) $\forall x \in S,\ x \in [x]$.
(2) $\forall x, y \in S$, *berlaku tepat salah satu dari* $[x] = [y]$ *atau* $[x] \cap [y] = \emptyset$.

BUKTI. (1): Pernyataan ini tidak lain adalah sifat refleksif dari $\cong$.

(2): Misalkan $z \in [x] \cap [y]$. Ini berarti $z \cong x$ dan $z \cong y$. Berdasarkan simetri, $x \cong z$; berdasarkan transitivitas, $x \cong y$.

Sekarang, jika $a \in [x]$ dan $b \in [y]$, maka $a \cong x$ dan $b \cong y$. Karena $x \cong y$, transitivitas memberi $a \cong y$, sehingga $a \in [y]$. Selain itu, simetri memberi $y \cong x$, lalu transitivitas memberi $b \cong x$, sehingga $b \in [x]$.

Oleh karena itu, $[x] \subseteq [y]$ dan $[y] \subseteq [x]$, sehingga $[x] = [y]$.

Argumen tersebut hanya menggunakan adanya suatu elemen $z \in [x] \cap [y]$. Jadi, jika $[x] \neq [y]$, haruslah $[x] \cap [y] = \emptyset$. Kedua kemungkinan itu tidak dapat berlaku sekaligus, sebab Bagian (1) menunjukkan bahwa setiap kelas ekuivalensi tidak kosong. □

CONTOH 2.4.3. Pada himpunan $S = \{(n, m) \mid n, m \in \mathbb{Z}, m \neq 0\}$, kita dapat mendefinisikan relasi $(a, b) \cong (c, d)$ jika $ad = cb$. Maka $S/\cong$ tidak lain adalah himpunan bilangan rasional, $\mathbb{Q}$!

Sekarang, mari kita khususkan konsep kelas ekuivalensi pada kongruensi.

PROPOSISI 2.4.4. *Untuk $n \in \mathbb{N}$, relasi pada $\mathbb{Z}$ yang didefinisikan oleh*

$$a \cong_n b \Leftrightarrow a \equiv b \pmod{n}$$

(yang akan kita tulis sebagai $a \cong b$ jika n jelas dari konteks) merupakan relasi ekuivalensi.

DEFINISI 2.4.5. Untuk $n \in \mathbb{N}$ dan $a \in \mathbb{Z}$, kelas ekuivalensi dari a menurut relasi ekuivalensi di atas disebut **kelas kongruensi dari** a **modulo** n dan ditulis $[a]_n$ (atau, dengan sedikit penyalahgunaan notasi, cukup $[a]$ jika n dipahami dari konteks). Himpunan kelas ekuivalensi $\mathbb{Z}/\cong_n$ disebut **bilangan bulat modulo** n dan ditulis $\mathbb{Z}/n\mathbb{Z}$ (atau, oleh sebagian penulis, $\mathbb{Z}/n$ atau $\mathbb{Z}_n$).

TEOREMA 2.4.6. *Untuk $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ mempunyai n elemen, dengan $0, \ldots, n-1$ sebagai wakil dari kelas-kelas ekuivalensi yang berbeda itu. Dengan kata lain,*

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \ldots, [n-1]_n\}.$$

BUKTI. Untuk $n \in \mathbb{N}$ dan $a \in \mathbb{Z}$, Algoritma Pembagian menyatakan bahwa terdapat pasangan tunggal $q, r \in \mathbb{Z}$ sedemikian sehingga $a = qn + r$ dan $0 \leq r < n$. Perhatikan bahwa $a \equiv r \pmod{n}$ atau, secara ekuivalen, $a \in [r]$. Jadi, setiap $a \in \mathbb{Z}$ merupakan anggota tepat satu kelas ekuivalensi $[r]$ untuk $r \in \{0, \ldots, n-1\}$. Karena setiap r tersebut berada dalam $[r]$, dan hanya dalam satu kelas semacam itu, kelas-kelas ekuivalensi $[0], \ldots, [n-1]$ semuanya berbeda. □

Hal menarik tentang $\mathbb{Z}/n\mathbb{Z}$ adalah bahwa kita dapat melakukan banyak operasi aritmetika bilangan bulat yang biasa di dalamnya; bahkan, terkadang kita dapat melakukan sedikit lebih banyak daripada biasanya.

DEFINISI 2.4.7. Untuk $n \in \mathbb{N}$ dan $\mathcal{C}, \mathcal{D} \in \mathbb{Z}/n\mathbb{Z}$, definisikan $\mathcal{C} + \mathcal{D} = [a + b]$ dan $\mathcal{C} \cdot \mathcal{D} = [a \cdot b]$, dengan a dan b masing-masing sebarang wakil dari kelas kongruensi $\mathcal{C}$ dan $\mathcal{D}$.

TEOREMA 2.4.8. *Operasi $+$ dan $\cdot$ pada $\mathbb{Z}/n\mathbb{Z}$ terdefinisi dengan baik. Artinya, kedua operasi itu tidak bergantung pada wakil kelas kongruensi yang dipilih.*

BUKTI. Misalkan $n \in \mathbb{N}$ dan $\mathcal{C}, \mathcal{D} \in \mathbb{Z}/n\mathbb{Z}$. Ambil $a, p, b, q \in \mathbb{Z}$ sedemikian sehingga $\mathcal{C} = [a] = [p]$ dan $\mathcal{D} = [b] = [q]$. Maka $p \equiv a \pmod{n}$ dan $q \equiv b \pmod{n}$. Berdasarkan Teorema 2.1.3, $a+b \equiv p+q \pmod{n}$ dan $a \cdot b \equiv p \cdot q \pmod{n}$, sehingga $[a+b] = [p+q]$ dan $[a \cdot b] = [p \cdot q]$. Jadi, baik $[a + b]$ maupun $[p + q]$ memberikan definisi yang sama bagi $\mathcal{C} + \mathcal{D}$, dan hal yang sama berlaku untuk $\mathcal{C} \cdot \mathcal{D}$. □

Operasi-operasi baru ini mempunyai sifat-sifat yang sangat baik.

TEOREMA 2.4.9. *Untuk $n \in \mathbb{N}$, penjumlahan dan perkalian pada $\mathbb{Z}/n\mathbb{Z}$*

(1) *bersifat komutatif dan asosiatif;*
(2) *perkalian bersifat distributif terhadap penjumlahan;*
(3) *kedua operasi mempunyai elemen identitas, yaitu $[0]$ untuk penjumlahan dan $[1]$ untuk perkalian;*
(4) *setiap elemen $\mathbb{Z}/n\mathbb{Z}$ mempunyai invers aditif, yaitu invers dari $[a]$ adalah $[-a]$ (atau $[n-a]$, nama lain bagi elemen yang sama); dan*

(5) *suatu elemen* $[a] \in \mathbb{Z}/n\mathbb{Z}$ *mempunyai invers multiplikatif* $[a]^{-1}$ *jika dan hanya jika* $\gcd(a, n) = 1$*; invers ini tunggal apabila ada.*

BUKTI. Diserahkan kepada pembaca. Perhatikan bahwa butir terakhir pada dasarnya merupakan Akibat 2.2.8 yang dinyatakan kembali dalam bahasa kelas kongruensi. □

Selain Akibat 2.2.8, banyak hasil kita sebelumnya juga dapat dinyatakan kembali dengan kelas kongruensi. Sebagian besar akan diserahkan kepada pembaca, tetapi berikut salah satu contohnya.

TEOREMA 2.4.10. *Untuk* $a, b \in \mathbb{Z}$ *dan* $n \in \mathbb{N}$*, misalkan* $d = \gcd(a, n)$*. Tinjau persamaan*

$$[a] \cdot x = [b]$$

dengan $x \in \mathbb{Z}/n\mathbb{Z}$*. Maka*

(1) *Jika* $d \nmid b$*, persamaan itu tidak mempunyai solusi.*
(2) *Jika* $d \mid b$*, persamaan itu mempunyai tepat* d *solusi dalam* $\mathbb{Z}/n\mathbb{Z}$*.*

BUKTI. Diserahkan kepada pembaca; pernyataan ini tidak lain adalah Teorema 2.2.4 dalam bentuk lain. □

Latihan untuk §2.4.

LATIHAN 2.4.1. Ketika bilangan rasional $\mathbb{Q}$ dideskripsikan seperti dalam Contoh 2.4.3, kita mendefinisikan penjumlahan dengan $[(n, m)]+[(p, q)] = [(nq+mp, mq)]$ dan perkalian dengan $[(n, m)] \cdot [(p, q)] = [(np, mq)]$, dengan $n, m, p, q \in \mathbb{Z}$ serta m dan q keduanya tidak nol. Buktikan padanan Teorema 2.4.8 untuk bentuk $\mathbb{Q}$ ini.

Apa saja identitas aditif dan multiplikatif dalam $\mathbb{Q}$ ini? Apakah setiap elemen (atau hampir setiap elemen) $\mathbb{Q}$ mempunyai invers aditif dan invers multiplikatif? Jika ya, berikan rumus bagi invers-invers tersebut; jika tidak, jelaskan alasannya.

LATIHAN 2.4.2. Nyatakan kembali Teorema Sisa Cina dengan kelas-kelas kongruensi dan *persamaan* dalam berbagai $\mathbb{Z}/n\mathbb{Z}$, bukan dengan kongruensi.

LATIHAN 2.4.3. Buktikan pernyataan-pernyataan dalam bagian ini yang buktinya "diserahkan kepada pembaca."

LATIHAN 2.4.4. Nyatakan dan buktikan versi kelas kongruensi dari setiap hasil tentang kongruensi dalam Bagian 2.1 dan Bagian 2.2 yang belum mempunyai versi dalam bagian ini.

2.5. Fungsi ϕ Euler

Euler membuat definisi berikut, dan definisi itu ternyata sangat berguna.

DEFINISI 2.5.1. Untuk $n \in \mathbb{N}$,

$$\phi(n) = \#\left(\{m \in \mathbb{Z} \mid 0 \leq m < n \text{ dan } \gcd(m,n) = 1\}\right) .$$

Dengan kata lain, $\phi(n)$ menghitung banyaknya bilangan bulat tak-negatif yang lebih kecil daripada n dan relatif prima dengan n.

Fungsi ini disebut **fungsi ϕ Euler**, atau **fungsi totient Euler**. (Dalam bahasa Inggris, "totient" berima dengan "quotient"; nama ini diberikan oleh matematikawan Inggris Sylvester.)

Berikut salah satu kegunaan fungsi tersebut.

TEOREMA 2.5.2. *Untuk $n \in \mathbb{N}$, $\phi(n)$ adalah banyaknya elemen $\mathbb{Z}/n\mathbb{Z}$ yang mempunyai invers multiplikatif.*

BUKTI. Pernyataan ini langsung mengikuti Bagian (5) dari Teorema 2.4.9. □

Satu fakta yang cukup mengejutkan tentang fungsi totient Euler adalah bahwa fungsi ini bersifat multiplikatif, setidaknya untuk bilangan-bilangan yang relatif prima.

TEOREMA 2.5.3. *Untuk $n, m \in \mathbb{N}$, jika $\gcd(n,m) = 1$, maka $\phi(nm) = \phi(n)\phi(m)$.*

BUKTI. Pernyataan ini merupakan penerapan Teorema Sisa Cina yang menarik, seperti yang akan kita lihat.

Tetapkan $n, m \in \mathbb{N}$ yang relatif prima. Untuk $k \in \mathbb{N}$, misalkan

$$(\mathbb{Z}/k\mathbb{Z})^* = \{x \in \mathbb{Z}/k\mathbb{Z} \mid x \text{ mempunyai invers multiplikatif}\}$$

sehingga $\phi(k) = \#((\mathbb{Z}/k\mathbb{Z})^*)$. (Notasi ini menyatakan *banyaknya elemen dalam himpunan* $(\mathbb{Z}/k\mathbb{Z})^*$.)

Sekarang, definisikan himpunan pasangan

$$(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* = \{(a,b) \mid a \in (\mathbb{Z}/n\mathbb{Z})^* \text{ dan } b \in (\mathbb{Z}/m\mathbb{Z})^*\} .$$

Perhatikan bahwa $\#((\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*) = \#((\mathbb{Z}/n\mathbb{Z})^*) \cdot \#((\mathbb{Z}/m\mathbb{Z})^*) = \phi(n)\phi(m)$, sebab setiap komponen pasangan dapat dipilih bebas dari himpunannya masing-masing. Jadi, banyaknya pasangan adalah hasil kali ukuran kedua himpunan. Oleh karena itu, jika kita dapat membuktikan bahwa $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ berkorespondensi secara bijektif dengan $(\mathbb{Z}/(nm)\mathbb{Z})^*$, maka

$$\phi(n)\phi(m) = \#\left((\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*\right) = \#((\mathbb{Z}/(nm)\mathbb{Z})^*) = \phi(nm)$$

seperti yang diinginkan, sebab himpunan-himpunan yang berkorespondensi secara bijektif mempunyai jumlah elemen yang sama.

Korespondensi tersebut diberikan oleh fungsi

$$\mathcal{F} : (\mathbb{Z}/(nm)\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* : [x]_{nm} \mapsto ([x]_n, [x]_m) \, .$$

Kita harus menunjukkan bahwa $\mathcal{F}$ terdefinisi dengan baik, injektif, dan surjektif. Pertama, $\mathcal{F}$ memang memetakan ke kodomain yang dinyatakan. Jika $[x]_{nm}$ mempunyai invers $[u]_{nm}$, maka $xu \equiv 1 \pmod{nm}$, sehingga $xu \equiv 1 \pmod{n}$ dan $xu \equiv 1 \pmod{m}$. Jadi, $[x]_n$ dan $[x]_m$ keduanya mempunyai invers multiplikatif.

Selanjutnya, keterdefinisian dengan baik berarti bahwa, untuk suatu $[x]_{nm}$, jika $y \in \mathbb{Z}$ merupakan wakil lain dari kelas kongruensi $[x]_{nm}$, maka $([x]_n, [x]_m) = ([y]_n, [y]_m)$. Dengan demikian, $\mathcal{F}$ ditentukan hanya oleh kelas $[x]_{nm}$, bukan oleh pilihan wakil x. Hal ini mudah dilihat: $y \in [x]_{nm}$ berarti $y \cong_{nm} x$, sehingga terdapat $k \in \mathbb{Z}$ sedemikian sehingga $y - x = k(nm) = (km)n = (kn)m$. Dua bentuk terakhir berarti $y \cong_n x$ dan $y \cong_m x$, sehingga $[x]_n = [y]_n$ dan $[x]_m = [y]_m$. Jadi, $\mathcal{F}$ terdefinisi dengan baik.

Sekarang, misalkan $x, y \in \mathbb{Z}$ memenuhi $\mathcal{F}([x]_{nm}) = \mathcal{F}([y]_{nm})$, yaitu $[x]_n = [y]_n$ dan $[x]_m = [y]_m$. Dengan demikian, $z = x - y \in \mathbb{Z}$ menyelesaikan sistem

$$\begin{aligned} z &\equiv 0 \pmod{n} \\ z &\equiv 0 \pmod{m} \, . \end{aligned}$$

Nilai $z = 0$ juga menyelesaikan sistem ini. Teorema Sisa Cina menyatakan bahwa solusi sistem tersebut tunggal modulo nm karena $\gcd(n, m) = 1$. Oleh karena itu, $x - y \equiv 0 \pmod{nm}$, sehingga $x \equiv y \pmod{nm}$. Jadi, $[x]_{nm} = [y]_{nm}$ dan $\mathcal{F}$ injektif.

Terakhir, ambil sebarang pasangan $([x]_n, [y]_m) \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ dan tinjau sistem

$$\begin{aligned} z &\equiv x \pmod{n} \\ z &\equiv y \pmod{m} \, , \end{aligned}$$

Karena $\gcd(n, m) = 1$, Teorema Sisa Cina memberikan suatu solusi $z \in \mathbb{Z}$.

Masih perlu ditunjukkan bahwa $[z]_{nm}$ mempunyai invers. Ambil $[u]_n = [x]_n^{-1}$ dan $[v]_m = [y]_m^{-1}$. Teorema Sisa Cina memberikan $w \in \mathbb{Z}$ yang memenuhi $w \equiv u \pmod{n}$ dan $w \equiv v \pmod{m}$. Akibatnya, $zw \equiv 1 \pmod{n}$ dan $zw \equiv 1 \pmod{m}$. Karena zw dan 1 merupakan solusi sistem yang sama, ketunggalan dalam Teorema Sisa Cina memberi $zw \equiv 1 \pmod{nm}$. Jadi, $[z]_{nm} \in (\mathbb{Z}/(nm)\mathbb{Z})^*$ dan $\mathcal{F}([z]_{nm}) = ([x]_n, [y]_m)$. Dengan demikian, $\mathcal{F}$ juga surjektif. $\square$

Latihan untuk §2.5.

LATIHAN 2.5.1. Hitunglah $\phi(n)$ untuk $n = 2, 3, 5, 7, 11, 13, 17$. Buatlah dugaan umum. Dapatkah Anda membuktikannya?

LATIHAN 2.5.2. Hitunglah $\phi(n)$ untuk $n = 2, 4, 8, 16, 32, 64$. Buatlah dugaan tentang $\phi(2^k)$ untuk $k \in \mathbb{N}$. Buktikan dugaan tersebut!

BAB 3

Bilangan Prima

Bilangan prima adalah atom-atom penyusun bilangan bulat komposit yang lebih rumit (molekul-molekul, dalam perumpamaan ini). Dalam bab ini, kita mempelajari beberapa sifat dasarnya, membuktikan Teorema Dasar Aritmetika, lalu melanjutkan ke Teorema Wilson.

3.1. Dasar-dasar dan Teorema Dasar Aritmetika

Pertama-tama, kita membuat definisi berikut.

DEFINISI 3.1.1. Bilangan $p \in \mathbb{N}$ disebut **prima** jika $p > 1$ dan satu-satunya bilangan asli yang membagi p adalah 1 dan p.

CONTOH 3.1.2. Beberapa bilangan prima adalah 2, 3, 5, 7, 11, 13, dan 17. Perhatikan bahwa 2 merupakan satu-satunya bilangan prima genap (jelas, sebab setiap bilangan genap lainnya merupakan kelipatan 2 dan karena itu tidak mungkin prima). Bilangan 2 memang mempunyai beberapa sifat tak lazim. Dalam bahasa Inggris ada permainan kata bahwa "2 is the oddest prime," sebab "oddest" dapat berarti "paling ganjil" maupun "paling aneh."

Bilangan prima terbesar yang diketahui manusia pada saat buku ini ditulis adalah

$$2^{57,885,161} - 1$$

yang dibuktikan prima pada Januari 2013 oleh program komputasi terdistribusi bernama **GIMPS** [*Great Internet Mersenne Prime Search*, Pencarian Besar-besaran Bilangan Prima Mersenne melalui Internet] yang berjalan pada ratusan komputer di seluruh Internet.

Sebagai pembanding, kita juga menggunakan istilah berikut.

DEFINISI 3.1.3. Bilangan $c \in \mathbb{N}$ yang lebih besar daripada 1 dan tidak prima disebut **komposit**.

Sejauh mana pemeriksaan langsung dengan cara kasar harus dilakukan untuk menentukan apakah suatu bilangan komposit?

TEOREMA 3.1.4. *Jika n komposit, maka n mempunyai pembagi positif d yang memenuhi $d \leq \sqrt{n}$.*

BUKTI. Misalkan n komposit. Maka n mempunyai suatu pembagi sejati $a \in \mathbb{N}$. Perhatikan bahwa $n = a \cdot \frac{n}{a}$, sehingga $\frac{n}{a} \in \mathbb{N}$ juga merupakan pembagi. Namun, a dan $\frac{n}{a}$ tidak mungkin keduanya lebih besar daripada $\sqrt{n}$, sebab jika demikian, kita akan memperoleh

$$n = a \cdot \frac{n}{a} > \sqrt{n} \cdot \sqrt{n} = n,$$

suatu kontradiksi. Jadi, setidaknya salah satu dari a atau $\frac{n}{a}$ merupakan pembagi d yang dijanjikan dalam pernyataan teorema. □

Lemma Euklides (Lemma 2.1.6) mempunyai bentuk yang sangat baik jika pembagi yang terlibat merupakan bilangan prima.

PROPOSISI 3.1.5. *Misalkan p prima dan $a, b \in \mathbb{Z}$. Jika $p \mid ab$, maka $p \mid a$ atau $p \mid b$.*

BUKTI. Perhatikan bahwa $\gcd(p, a) \mid p$. Karena p prima, $\gcd(p, a)$ bernilai 1 atau p. Selain itu, $\gcd(a, p) \mid a$, sehingga $p \mid a$ atau $\gcd(a, p) = 1$. Jika $p \mid a$, pembuktian selesai. Jika tidak, $\gcd(a, p) = 1$, sehingga Lemma Euklides 2.1.6 menyatakan bahwa $p \mid b$. □

Bentuk yang lebih umum dari hasil ini adalah sebagai berikut.

AKIBAT 3.1.6. *Misalkan p prima, $k \in \mathbb{N}$, dan $a_1, \ldots, a_k \in \mathbb{Z}$. Jika $p \mid a_1 \ldots a_k$, maka p membagi setidaknya satu dari bilangan a_j.*

BUKTI. Diserahkan kepada pembaca (gunakan induksi pada k). □

Hasil ini membawa kita pada teorema yang namanya sangat sesuai berikut.

TEOREMA 3.1.7. ***Teorema Dasar Aritmetika:*** *Misalkan $n \in \mathbb{N}$, $n \geq 2$. Maka terdapat $k \in \mathbb{N}$ dan bilangan-bilangan prima $p_1, \ldots, p_k$ sedemikian sehingga $n = p_1 \ldots p_k$. Lebih lanjut, jika $l \in \mathbb{N}$ dan $q_1, \ldots, q_l$ juga bilangan-bilangan prima yang memenuhi $n = q_1 \ldots q_l$, maka $l = k$ dan faktorisasi dengan faktor-faktor q hanya merupakan penyusunan ulang dari faktorisasi dengan faktor-faktor p.*

BUKTI. Untuk bagian eksistensi, kita menggunakan Prinsip Kedua Induksi Matematika. Pernyataan umum yang akan dibuktikan adalah $\forall n \in \mathbb{Z},\ n > 1 \Rightarrow S(n)$, dengan $S(n)$ menyatakan "terdapat $k \in \mathbb{N}$ dan bilangan-bilangan prima $p_1, \ldots, p_k$ sedemikian sehingga $n = p_1 \ldots p_k$."

Sebagai langkah dasar, ambil $n = 2$. Pilihan $k = 1$ dan $p_1 = 2$ memenuhi pernyataan tersebut.

Sekarang, anggap $S(r)$ benar untuk setiap bilangan bulat r yang memenuhi $1 < r < n$. Jika n prima, pilihan $k = 1$ dan $p_1 = n$ memenuhi pernyataan. Sebaliknya, misalkan n komposit dengan pembagi sejati d. Maka $1 < d < n$ dan $1 < \frac{n}{d} < n$. Berdasarkan hipotesis induksi, terdapat $k, k' \in \mathbb{N}$ dan bilangan-bilangan prima $p_1, \ldots, p_k, p'_1, \ldots, p'_{k'}$ sedemikian sehingga $d = p_1 \ldots p_k$ dan $\frac{n}{d} = p'_1 \ldots p'_{k'}$. Dengan demikian, n merupakan hasil kali

$$n = p_1 \ldots p_k \cdot p'_1 \ldots p'_{k'}$$

dari $k+k'$ bilangan prima. Jadi, $S(n)$ juga benar; dengan demikian, faktorisasi prima selalu ada.

Sekarang, misalkan $n \in \mathbb{Z}$, $n > 1$, mempunyai dua faktorisasi prima, yakni terdapat $k, l \in \mathbb{N}$ dan bilangan-bilangan prima $p_1, \ldots, p_k$ serta $q_1, \ldots, q_l$ sedemikian sehingga

$$p_1 \ldots p_k = n = q_1 \ldots q_l \ .$$

Jelas bahwa p_1 membagi ruas kiri, sehingga p_1 juga membagi $q_1 \ldots q_l$. Berdasarkan Akibat 3.1.6, p_1 membagi salah satu q_j. Karena p_1 dan q_j keduanya prima, haruslah $p_1 = q_j$. Setelah membatalkan p_1 pada ruas kiri dan q_j pada ruas kanan, kita memperoleh

$$\prod_{i=2}^{k} p_i = \frac{n}{p_1} = \prod_{\substack{1 \le i \le l \\ i \ne j}} q_i \ ,$$

dengan hasil kali kosong ditafsirkan sebagai 1. Lanjutkan pembatalan dengan cara yang sama. Salah satu daftar faktor tidak mungkin habis lebih dahulu, sebab hal itu akan membuat hasil kali satu atau lebih bilangan prima pada ruas lain sama dengan 1, yang mustahil. Jadi, kedua daftar mempunyai panjang yang sama, dan faktor-faktornya sama hingga urutan. Inilah ketunggalan yang dinyatakan dalam teorema. $\square$

Latihan untuk §3.1.

LATIHAN 3.1.1. Berikan semua perincian bukti Akibat 3.1.6.

LATIHAN 3.1.2. Nyatakan dan buktikan suatu teorema tentang faktorisasi prima dari bilangan $a, b \in \mathbb{N}$ dan dari faktor persekutuan terbesarnya.

LATIHAN 3.1.3. Bilangan $n \in \mathbb{N}$ disebut *bebas kuadrat* jika tidak habis dibagi oleh kuadrat bilangan asli apa pun selain 1. Buktikan bahwa n bebas kuadrat jika dan hanya jika n merupakan hasil kali berhingga dari bilangan-bilangan prima yang berbeda, dengan hasil kali kosong diizinkan dan bernilai 1.

3.2. Teorema Wilson

Dalam bagian ini, kita membuktikan sebuah teorema menarik yang biasanya dinamai menurut seorang matematikawan Inggris abad ke-18 ... meskipun teorema itu sebenarnya pertama kali dinyatakan oleh Ibn al-Haytham hampir 800 tahun sebelumnya.

Pertama, kita memerlukan lemma berikut.

LEMA 3.2.1. *Misalkan p bilangan prima. Maka $n \in \mathbb{N}$ merupakan invers bagi dirinya sendiri modulo p jika dan hanya jika $p \mid n+1$ atau $p \mid n-1$, yaitu jika dan hanya jika $n \equiv \pm 1 \pmod{p}$.*

BUKTI. Misalkan p bilangan prima dan $n \in \mathbb{N}$ merupakan invers bagi dirinya sendiri modulo p. Artinya, $n^2 = n \cdot n \equiv 1 \pmod{p}$. Menurut definisi, $p \mid n^2 - 1 = (n+1)(n-1)$. Berdasarkan Proposisi 3.1.5, hal ini berarti $p \mid n+1$ atau $p \mid n-1$.

Sebaliknya, andaikan $n \equiv 1 \pmod{p}$ atau $n \equiv -1 \pmod{p}$. Berdasarkan Teorema 2.1.3, $n^2 \equiv (\pm 1)^2 = 1 \pmod{p}$, sehingga n merupakan invers bagi dirinya sendiri modulo p. □

Lemma ini merupakan langkah kunci dalam pembuktian teorema berikut.

TEOREMA 3.2.2. ***Teorema Wilson*** *Diberikan $p \in \mathbb{N}$ dengan $p \geq 2$, bilangan p prima jika dan hanya jika $(p-1)! \equiv -1 \pmod{p}$.*

BUKTI. Andaikan p prima. Jika $p = 2$, maka $(p-1)! = 1 \equiv -1 \pmod{2}$, sehingga kesimpulan yang diinginkan berlaku. Sekarang andaikan p ganjil. Menurut Akibat 2.2.8, setiap bilangan $2, \ldots, p-2$ mempunyai invers modulo p, dan menurut Lemma 3.2.1, tidak satu pun di antaranya merupakan invers bagi dirinya sendiri. Oleh karena itu, bilangan-bilangan tersebut dapat dikelompokkan menjadi $(p-3)/2$ pasangan invers. Dengan menyisakan hanya 1 dan $(p-1)$, kita memperoleh

$$(p-1)! \equiv 1 \cdot 1^{(p-3)/2} \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}.$$

Sebaliknya, andaikan $p \in \mathbb{N}$ memenuhi $p \geq 2$ dan $(p-1)! \equiv -1 \pmod{p}$. Kongruensi ini dapat ditulis kembali sebagai $(p-1)! + 1 \equiv 0 \pmod{p}$, atau $p \mid ((p-1)! + 1)$.

Sekarang, misalkan $d \in \mathbb{N}$ pembagi p dengan $d \neq p$. Dengan demikian, d merupakan salah satu bilangan dalam hasil kali $(p-1)!$, sehingga $d \mid (p-1)!$. Selain itu, karena $d \mid p$ dan $p \mid ((p-1)! + 1)$, berlaku pula $d \mid ((p-1)! + 1)$. Oleh Teorema 1.3.9,

$$d \mid ((p-1)! + 1) - (p-1)! = 1,$$

yang berarti $d = 1$.

Dengan kata lain, setiap pembagi $d \in \mathbb{N}$ dari p haruslah p atau 1; jadi, p prima. □

CONTOH 3.2.3. Mari kita telusuri salah satu arah pembuktian untuk kasus sederhana, misalnya $p = 7$. Mula-mula, kita mencari pasangan invers di antara bilangan $2, \ldots, 5$

(dengan mencoba langsung dalam kasus kecil ini): $2 \cdot 4 \equiv 1 \pmod 7$ dan $3 \cdot 5 \equiv 1 \pmod 7$. Artinya, $2^{-1} \equiv 4$ (atau $4^{-1} \equiv 2$) dan $3^{-1} \equiv 5$ (atau $5^{-1} \equiv 3$).

Kemudian,

$$(p-2)! = 5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = (5 \cdot 3) \cdot (4 \cdot 2) \equiv 1 \cdot 1 \equiv 1 \pmod 7,$$

yang selanjutnya memberikan

$$(p-1)! = 6! = 6 \cdot 5! \equiv 6 \cdot 1 \equiv 6 \equiv 7 - 1 \equiv -1 \pmod 7.$$

Perhatikan bahwa Teorema Wilson dapat digunakan untuk membuat uji keprimaan: periksa apakah suatu bilangan n memenuhi $(n-1)! \equiv -1 \pmod n$; jika ya, maka n prima. Uji ini sama sekali tidak praktis, tetapi inilah contoh pertama kita tentang kongruensi komputasional sederhana yang melibatkan suatu bilangan bulat dan dapat memberi tahu kita bahwa bilangan tersebut prima.

3.3. Orde Multiplikatif dan Penerapannya

Dalam bagian ini, kita membuktikan dua hasil yang sangat berguna, yaitu Teorema Euler dan Teorema Kecil Fermat (suatu kasus khusus dari Teorema Euler). Namun, kita tidak mengikuti strategi pembuktian Euler dan Fermat, melainkan menggunakan pendekatan yang terinspirasi oleh aljabar abstrak dan Teorema Lagrange di bidang tersebut.

Pertama, kita memerlukan definisi berikut.

DEFINISI 3.3.1. Andaikan $n \in \mathbb{N}$ dan $a \in \mathbb{Z}$ memenuhi $n \geq 2$ dan $\gcd(a, n) = 1$. Kita mendefinisikan **orde multiplikatif** a **modulo** n (cukup disebut *orde* apabila kata *multiplikatif* dan nilai n dapat dipahami dari konteks) sebagai bilangan terkecil $k \in \mathbb{N}$ sedemikian sehingga $a^k \equiv 1 \pmod{n}$. Orde a modulo n ditulis $\mathrm{ord}_n(a)$.

Mari kita memeriksa sesuatu yang semestinya selalu diperiksa untuk sebuah definisi baru.

PROPOSISI 3.3.2. *Diberikan $n \in \mathbb{N}$ dan $a \in \mathbb{Z}$ yang relatif prima, dengan $n \geq 2$, maka $\mathrm{ord}_n(a)$ terdefinisi dengan baik.*

BUKTI. Masalah yang mungkin muncul dalam definisi $\mathrm{ord}_n(a)$ adalah tidak adanya nilai $k \in \mathbb{N}$ yang memenuhi $a^k \equiv 1 \pmod{n}$.

Namun, perhatikan bahwa ini adalah sebuah kongruensi, sehingga kita sebenarnya hanya memperhatikan kelas kongruensi dari elemen-elemen a^k.

Perhatikan $\{[a^p]_n \mid p \in \mathbb{N}\}$ dan bayangkan kita memasukkan setiap bilangan asli $p \in \mathbb{N}$ ke dalam kotak yang ditentukan oleh kelas kongruensi $[a^p] \in \mathbb{Z}/n\mathbb{Z}$. Karena $\mathbb{N}$ mempunyai tak berhingga banyak elemen, sedangkan $\mathbb{Z}/n\mathbb{Z}$ hanya mempunyai n elemen—atau n *kotak*—maka menurut Prinsip Sarang Merpati (Teorema 1.1.2) terdapat dua (bahkan tak berhingga banyak pasangan) nilai berbeda $p, q \in \mathbb{N}$ yang masuk ke kotak yang sama. Artinya, $[a^p] = [a^q]$. Tanpa mengurangi keumuman, andaikan $p > q$, sehingga $p - q \in \mathbb{N}$.

Kita mengetahui bahwa $\gcd(a, n) = 1$, sehingga, berdasarkan Akibat 2.2.8, invers a^{-1} ada modulo n. Oleh karena itu,

$$a^{p-q} \equiv a^p\,(a^{-1})^q \equiv a^q\,(a^{-1})^q \equiv a^0 \equiv 1 \pmod{n}.$$

Di bagian tengah kongruensi ini, kita mengganti a^p dengan a^q karena $[a^p] = [a^q]$, yang berarti $a^p \equiv a^q \pmod{n}$. Jadi, himpunan semua $k \in \mathbb{N}$ yang memenuhi $a^k \equiv 1 \pmod{n}$ tidak kosong. Orde adalah nilai terkecil dalam himpunan tersebut, dan keberadaannya dijamin oleh Prinsip Keterurutan Baik. □

Berikut adalah sebuah teorema dari aljabar abstrak (Teorema Lagrange) yang dinyatakan dalam konteks kita saat ini.

TEOREMA 3.3.3. *Diberikan $n \in \mathbb{N}$ dan $a \in \mathbb{Z}$ yang relatif prima, dengan $n \geq 2$, maka $\mathrm{ord}_n(a) \mid \phi(n)$.*

BUKTI. Mulailah dengan memperhatikan kelas-kelas kongruensi $[a], [a^2], [a^3], \ldots$. Kelas-kelas ini berlanjut hingga $[a^{\mathrm{ord}_n(a)}] = [1]$, lalu mulai berulang. Berdasarkan keminimalan $\mathrm{ord}_n(a)$, kelas-kelas sebelum pengulangan itu berbeda satu sama lain. Jadi, himpunan

$$\langle a \rangle = \{[a^j] \mid j \in \mathbb{N}, j \leq \mathrm{ord}_n(a)\}$$

terdiri atas $\mathrm{ord}_n(a)$ elemen dari $\mathbb{Z}/n\mathbb{Z}$. Dalam teori grup, himpunan $\langle a \rangle$ disebut *subgrup siklik dari* $(\mathbb{Z}/n\mathbb{Z})^*$ *yang dibangkitkan oleh* a. Perhatikan bahwa $a^{\mathrm{ord}_n(a)} \equiv 1 \pmod{n}$, sehingga $[1] \in \langle a \rangle$. Selain itu, jika a^{-1} adalah invers a modulo n, maka $(a^{-1})^k$ adalah invers a^k untuk setiap $k \in \mathbb{N}$. Dengan demikian, $\langle a \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^*$.

Untuk menyelesaikan pembuktian, kita akan menunjukkan bahwa $(\mathbb{Z}/n\mathbb{Z})^*$ tersusun atas sejumlah bagian, katakanlah m bagian, yang kita sebut *koset*. Setiap koset berkorespondensi secara bijektif dengan $\langle a \rangle$, sehingga masing-masing mempunyai $\mathrm{ord}_n(a)$ elemen. Oleh karena itu,

$$m \cdot \mathrm{ord}_n(a) = \#\left((\mathbb{Z}/n\mathbb{Z})^*\right) = \phi(n),$$

dan hasil yang diinginkan pun mengikuti.

Sebuah *koset dari* $\langle a \rangle$ adalah himpunan berbentuk

$$x\langle a \rangle = \{[x] \cdot [a^j] = [x\, a^j] \mid j \in \mathbb{N}, j \leq \mathrm{ord}_n(a)\}$$

dengan $[x] \in (\mathbb{Z}/n\mathbb{Z})^*$. Kita telah melihat bahwa $[1] \in \langle a \rangle$. Jadi, untuk setiap $[x] \in (\mathbb{Z}/n\mathbb{Z})^*$, berlaku $[x] \in x\langle a \rangle$. Artinya, setiap kelas kongruensi dalam $(\mathbb{Z}/n\mathbb{Z})^*$ berada di suatu koset. Karena setiap koset juga merupakan subhimpunan $(\mathbb{Z}/n\mathbb{Z})^*$, kita mempunyai

$$(\mathbb{Z}/n\mathbb{Z})^* = \bigcup_{[x] \in (\mathbb{Z}/n\mathbb{Z})^*} x\langle a \rangle .$$

Setiap koset $x\langle a \rangle$ memang berkorespondensi secara bijektif dengan $\langle a \rangle$. Bijeksinya adalah pemetaan $f_x : \langle a \rangle \to x\langle a \rangle$ yang didefinisikan oleh $f_x([a^j]) = [xa^j]$ untuk $j \in \mathbb{N}$ dengan $j \leq \mathrm{ord}_n(a)$. Pemetaan ini mempunyai invers berupa perkalian dengan kelas $[x^{-1}]$, yang berasal dari invers x modulo n.

Sekarang, misalkan $x\langle a \rangle$ dan $y\langle a \rangle$ adalah dua koset. Kita akan menunjukkan bahwa keduanya sama atau saling lepas. Andaikan $x\langle a \rangle \cap y\langle a \rangle \neq \emptyset$. Maka terdapat $[z] \in x\langle a \rangle \cap y\langle a \rangle$, sehingga terdapat $j, k \in \mathbb{N}$ dengan $j, k \leq \mathrm{ord}_n(a)$ dan $[xa^j] = [z] = [ya^k]$. Dengan kata lain,

$$xa^j \equiv ya^k \pmod{n}.$$

Tanpa mengurangi keumuman, andaikan $j \leq k$. Dengan mengalikan kedua ruas kongruensi tersebut dengan $(a^{-1})^j$, kita memperoleh $x \equiv ya^{k-j} \pmod{n}$. Karena itu, setiap elemen $[xa^t] \in x\langle a \rangle$ dapat ditulis sebagai $[ya^{t+k-j}]$; dengan mengurangi pangkatnya modulo $\mathrm{ord}_n(a)$ (dan mewakili sisa nol dengan $\mathrm{ord}_n(a)$), kelas ini berada di $y\langle a \rangle$. Jadi, $x\langle a \rangle \subseteq y\langle a \rangle$. Kedua koset mempunyai banyak elemen berhingga yang sama, yaitu $\mathrm{ord}_n(a)$, sehingga keduanya sama. Dengan demikian, dua koset mana pun sama atau saling

lepas, dan koset-koset tersebut membentuk partisi $(\mathbb{Z}/n\mathbb{Z})^*$. Persamaan kardinalitas di atas kini membuktikan bahwa $\mathrm{ord}_n(a) \mid \phi(n)$. □

Pembuktian tadi cukup panjang, tetapi sekarang kita dapat memperoleh Teorema Kecil Fermat dan Teorema Euler yang terkenal itu dengan sangat mudah.

TEOREMA 3.3.4. ***Teorema Euler*** *Misalkan $a \in \mathbb{Z}$ dan $n \in \mathbb{N}$ memenuhi $\gcd(a, n) = 1$. Maka $a^{\phi(n)} \equiv 1 \pmod{n}$.*

BUKTI. Jika $n = 1$, hasilnya langsung berlaku karena semua bilangan bulat kongruen modulo 1. Sekarang andaikan $n \geq 2$. Teorema sebelumnya, Teorema 3.3.3, menyatakan bahwa $\mathrm{ord}_n(a) \mid \phi(n)$. Jadi, terdapat $m \in \mathbb{N}$ sedemikian sehingga $m \cdot \mathrm{ord}_n(a) = \phi(n)$. Berdasarkan definisi orde,

$$a^{\phi(n)} \equiv a^{m \,\mathrm{ord}_n(a)} \equiv \left(a^{\mathrm{ord}_n(a)}\right)^m \equiv 1^m \equiv 1 \pmod{n}.$$

□

AKIBAT 3.3.5. ***Teorema Kecil Fermat*** *Jika p prima dan $a \in \mathbb{Z}$ memenuhi $\gcd(p, a) = 1$, maka $a^{p-1} \equiv 1 \pmod{p}$.*

BUKTI. Kita telah melihat bahwa $\phi(p) = p-1$ untuk setiap bilangan prima p, sehingga hasil ini langsung mengikuti dari Teorema Euler. □

Teorema Kecil Fermat terkadang dijumpai dalam bentuk lain berikut.

TEOREMA 3.3.6. *Jika p prima, maka untuk setiap $a \in \mathbb{Z}$ berlaku $a^p \equiv a \pmod{p}$.*

BUKTI. Jika $\gcd(a, p) = 1$, maka, berdasarkan Teorema Kecil Fermat, $a^{p-1} \equiv 1 \pmod{p}$. Mengalikan kedua ruas kongruensi ini dengan a menghasilkan kesimpulan yang diinginkan.

Sebaliknya, jika $\gcd(a, p) \neq 1$, maka $\gcd(a, p) = p$, sebab FPB tersebut merupakan pembagi bilangan prima p. FPB itu juga membagi a, sehingga $p \mid a$. Akibatnya, a dan semua pangkat positifnya kongruen dengan 0 modulo p, dan $a^p \equiv 0 \equiv a \pmod{p}$. □

Latihan untuk §3.3.

LATIHAN 3.3.1. Berapakah sisa pembagian $15!$ oleh 17, dan berapakah sisa pembagian $2 \cdot (26!)$ oleh 29?

LATIHAN 3.3.2. Kita tahu bahwa 17 prima (bilangan yang luar biasa, bukan?). Namun, untuk memastikannya, gunakan Teorema Wilson untuk membuktikan bahwa 17 prima.

LATIHAN 3.3.3. Bisakah kita membuat uji keprimaan berdasarkan Teorema Kecil Fermat? Jika bisa, apakah uji itu lebih baik (lebih efisien) daripada uji berdasarkan Teorema Wilson? Bagaimana cara kerjanya? Tuliskan pernyataan formal yang jelas untuk uji keprimaan yang Anda usulkan.

Jika Anda menguasai suatu bahasa pemrograman, tulislah kode untuk mencoba uji keprimaan tersebut. Jika tidak (atau, bagaimanapun juga, setelah menulis program), lakukan sedikit penelitian untuk mengetahui apakah pertanyaan ini sudah pernah dikaji dan, jika ya, apa kesimpulannya. Berikan pernyataan formal uji tersebut beserta hasil formal yang menjelaskan keampuhannya, atau berikan contoh penyangkal bagi uji Anda yang ditemukan dalam literatur.

LATIHAN 3.3.4. Andaikan p bilangan prima ganjil. Buktikan bahwa jika kongruensi kuadrat $x^2 + 1 \equiv 0 \pmod{p}$ mempunyai solusi, maka $p \equiv 1 \pmod{4}$. *[Petunjuk: Terapkan Teorema Kecil Fermat pada suatu solusi a dari kongruensi tersebut, lalu kalikan dan bagi pangkatnya dengan 2.]*

3.4. Pendekatan Lain terhadap Teorema Kecil Fermat dan Teorema Euler

Ada cara lain untuk memahami teorema-teorema ini. Kita akan menjelaskannya di sini karena cara tersebut berguna untuk melengkapi pemahaman kita tentang perkalian dalam $\mathbb{Z}/n\mathbb{Z}$.

Kali ini, kita akan membahas kedua teorema dalam urutan yang berlawanan dengan urutan sebelumnya; urutan ini justru lebih sesuai dengan sejarahnya.

TEOREMA 3.4.1. ***Teorema Kecil Fermat, Ditinjau Kembali*** *Jika p prima dan $a \in \mathbb{Z}$ memenuhi $\gcd(p, a) = 1$, maka $a^{p-1} \equiv 1 \pmod{p}$.*

BUKTI. Kita mulai dengan membuktikan bahwa himpunan

$$M_a = \{[0]_p, [a]_p, [2a]_p, \ldots, [(p-1)a]_p\}$$

yang terdiri atas kelipatan-kelipatan $[a]_p$ dalam $\mathbb{Z}/p\mathbb{Z}$ mempunyai p elemen.

Di antara tanda $\{$ dan $\}$ hanya tercantum p kelas kongruensi, sehingga himpunan tersebut tidak mungkin mempunyai lebih dari p elemen.

Sekarang, ambil dua elemen dari himpunan ini, yaitu $[ja]_p$ dan $[ka]_p$, dengan $0 \leq j, k < p$, dan andaikan keduanya sama. Artinya, $ja \equiv ka \pmod{p}$, atau $p \mid (j-k)a$. Menurut Proposisi 3.1.5, berlaku $p \mid (j-k)$ atau $p \mid a$. Karena $\gcd(p, a) = 1$, tidak mungkin $p \mid a$. Jadi, $p \mid (j-k)$.

Karena $0 \leq j, k < p$, kita mempunyai $-p < j - k < p$, dan satu-satunya kelipatan p dalam rentang ini adalah 0. Oleh karena itu, $j = k$. Semua elemen dalam deskripsi M_a di atas berbeda, sehingga $\#(M_a) = p$. Kita juga telah mengetahui bahwa $\mathbb{Z}/p\mathbb{Z}$ mempunyai p elemen; jadi, M_a hanyalah cara lain untuk mendeskripsikan $\mathbb{Z}/p\mathbb{Z}$.

Sebagai langkah berikutnya, kalikan semua elemen tak nol dari M_a, atau sama saja, semua elemen tak nol dari $\mathbb{Z}/p\mathbb{Z}$:

$$a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod{p}.$$

Dengan menyusun ulang faktor-faktornya, kita memperoleh

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p},$$

atau $p \mid (a^{p-1} - 1)(p-1)!$. Karena p prima, berlaku $\gcd(p, (p-1)!) = 1$. Berdasarkan Proposisi 3.1.5, kita memperoleh $p \mid a^{p-1} - 1$. Dengan kata lain, $a^{p-1} \equiv 1 \pmod{p}$, seperti yang diinginkan. □

Pembuktian di atas cukup mirip dengan pembuktian Teorema Kecil Fermat yang diberikan oleh Euler. Sebenarnya, Fermat sama sekali tidak memberikan bukti, seperti halnya "Teorema" Terakhir Fermat yang terkenal itu. Strategi yang sangat mirip juga dapat digunakan untuk membuktikan Teorema Euler sendiri.

TEOREMA 3.4.2. ***Teorema Euler, Ditinjau Kembali*** *Misalkan $a \in \mathbb{Z}$ dan $n \in \mathbb{N}$ memenuhi $\gcd(a, n) = 1$. Maka $a^{\phi(n)} \equiv 1 \pmod{n}$.*

BUKTI. Jika $n = 1$, kesimpulannya langsung berlaku karena semua bilangan bulat kongruen modulo 1. Sekarang andaikan $n \geq 2$. Ingat bahwa himpunan elemen yang dapat dibalik secara multiplikatif dalam $\mathbb{Z}/n\mathbb{Z}$ dapat ditulis sebagai

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[b_1]_n, \ldots, [b_{\phi(n)}]_n\},$$

dengan bilangan-bilangan $b_1, \ldots, b_{\phi(n)}$ yang semuanya relatif prima terhadap n dan memenuhi $1 \leq b_1 < \cdots < b_{\phi(n)} < n$.

Kita mengklaim bahwa $(\mathbb{Z}/n\mathbb{Z})^*$ juga dapat dideskripsikan sebagai himpunan

$$M_a^* = \left\{[b_1 a]_n, \ldots, [b_{\phi(n)} a]_n\right\}.$$

Pertama, karena setiap b_j relatif prima terhadap n, demikian pula a, maka $b_j a$ juga relatif prima terhadap n. Setiap bilangan prima yang membagi $b_j a$ membagi b_j atau a, dan tidak ada bilangan prima semacam itu yang juga membagi n. Jadi, $M_a^* \subseteq (\mathbb{Z}/n\mathbb{Z})^*$.

Selanjutnya, jika $[b_j a]_n = [b_k a]_n$ untuk $1 \leq j, k \leq \phi(n)$, maka $n \mid (b_j - b_k)a$. Berdasarkan Lemma Euklides 2.1.6 , karena $\gcd(a, n) = 1$, kita harus mempunyai $n \mid (b_j - b_k)$.

Namun, karena $1 \leq b_1 < \cdots < b_{\phi(n)} < n$, berlaku $-n + 1 < b_j - b_k < n - 1$, dan satu-satunya kelipatan n dalam rentang ini adalah 0. Jadi, $b_j = b_k$, sehingga semua elemen dalam deskripsi M_a^* di atas berbeda. Himpunan M_a^* mempunyai $\phi(n)$ elemen dan merupakan subhimpunan $(\mathbb{Z}/n\mathbb{Z})^*$, yang juga hanya mempunyai $\phi(n)$ elemen. Oleh karena itu, $M_a^* = (\mathbb{Z}/n\mathbb{Z})^*$.

Seperti dalam pembuktian sebelumnya, hasil kali semua elemen M_a^* harus sama dengan hasil kali semua elemen $(\mathbb{Z}/n\mathbb{Z})^*$:

$$b_1 a \cdot \cdots \cdot b_{\phi(n)} a \equiv b_1 \cdot \cdots \cdot b_{\phi(n)} \pmod{n}.$$

Dengan mengelompokkan ulang faktor-faktornya, kita memperoleh

$$a^{\phi(n)} b_1 \cdot \cdots \cdot b_{\phi(n)} \equiv b_1 \cdot \cdots \cdot b_{\phi(n)} \pmod{n}.$$

Semua b_j mempunyai invers modulo n. Dengan mengalikan kedua ruas secara berturut-turut dengan invers-invers tersebut, kita memperoleh

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

yang menyelesaikan pembuktian Teorema Euler. □

Latihan untuk §3.4.

LATIHAN 3.4.1. Misalkan n, a, dan $b_1, \ldots, b_{\phi(n)}$ seperti dalam pembuktian Teorema Euler. Tunjukkan bahwa $b_1 \cdot \cdots \cdot b_{\phi(n)} \equiv \pm 1 \pmod{n}$.

BAB 4

Kriptologi

Berikut adalah beberapa akar kata Yunani:

kryptos, $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$: rahasia, tersembunyi
logos, $\lambda\acute{o}\gamma o\varsigma$: kata, kajian, tuturan
graph, $\gamma\rho\acute{\alpha}\varphi\omega$: menulis, tertulis

Dari akar-akar kata ini (dan beberapa akar lainnya), bahasa Inggris membentuk kata-kata yang kemudian diserap ke dalam bahasa Indonesia sebagai berikut.

kriptosistem: sekumpulan algoritme untuk melindungi rahasia
kriptografi: pekerjaan untuk membuat kriptosistem
kriptanalisis: pekerjaan untuk menembus perlindungan suatu kriptosistem
kriptologi: gabungan kriptografi dan kriptanalisis,
yang sering disingkat menjadi *kripto*.

Perhatikan bahwa kata *kriptografi* sering (tetapi kurang tepat!) digunakan sebagai sinekdoke untuk *kriptologi*. Hal ini mirip dengan penyalahgunaan kata *peretas* (*hacker*) yang juga dipahami secara luas. Kita akan berusaha menggunakan istilah-istilah tersebut dengan lebih cermat.

Dengan pemahaman itu, kita memulai bab ini dengan sedikit *kriptologi* dasar. Teori bilangan hanya akan muncul sedikit, tetapi kita akan memperkenalkan sejumlah istilah serta contoh sederhana kriptografi dan kriptanalisis yang bersesuaian. Penekanannya ada pada sistem-sistem bersejarah yang sudah tidak layak digunakan pada zaman modern. Bab-bab selanjutnya akan segera beralih ke teknik kripto modern yang berlandaskan teori bilangan.

4.1. Sedikit Sejarah Spekulatif

Mungkin suatu bentuk tipu daya sudah ada sebelum bahasa. Banyak hewan peliharaan tentu pernah berpura-pura tidak bersalah meskipun bukti keterlibatannya dalam pencurian kudapan sangat jelas. Bahkan ahli apiologi mungkin tidak tahu apakah sejumlah lebah malas mengarang cerita tentang perjalanan jauh menuju hamparan bunga baru ketika sang ratu meminta pertanggungjawaban.

Namun, di antara *Homo sapiens*, kebohongan mungkin sudah muncul segera setelah bahasa muncul. Tentu saja, ketika dua orang bertatap muka, kedua pihak masih mempunyai kendali tertentu: pendengar dapat mencoba menilai apakah pembicara dapat dipercaya; keduanya dapat menilai sendiri identitas lawan bicaranya lalu memilih apa yang ingin dibagikan; dan kata-kata pembicara bergerak langsung dari bibirnya ke telinga pendengar tanpa dapat diubah maknanya di tengah jalan (jika kita mengabaikan kebisingan sekitar dan sebagainya).

Banyak hal berubah setelah tulisan ditemukan lebih dari 5.000 tahun yang lalu. Kata-kata yang dibekukan dalam bentuk fisik, beserta gagasan yang diwakilinya, dapat diambil dan dibagikan kepada berbagai pihak selain pihak yang semula hendak dihubungi penulis. Selain itu, jika penulis tidak dapat menyerahkan karyanya langsung kepada pembaca yang dituju dan tulisan tersebut harus beredar sendiri untuk sementara waktu, kedua pihak tidak lagi dapat memastikan bahwa lawan komunikasinya benar-benar memiliki identitas yang dinyatakan dalam tulisan, ataupun bahwa simbol-simbol tertulis itu tidak berubah sejak dituliskan oleh pihak lainnya.

Mari kita merumuskan beberapa persoalan *keamanan informasi* (sebutannya sekarang) dalam konteks sebuah pesan yang hendak dikirim oleh seseorang bernama *Alice* kepada seseorang bernama *Bob*. Dalam drama kecil kita, lingkungan yang mungkin mengganggu dan terlalu mencampuri urusan orang lain diperankan oleh *Eve*. Secara tradisi, kita langsung memilih tokoh dengan nama yang diawali huruf *E* untuk melambangkan *environment* (lingkungan) sekaligus seseorang yang mungkin menjadi *eavesdropper* (penyadap)[1].

Berikut adalah beberapa istilah dasar.

DEFINISI 4.1.1. **Kerahasiaan** berarti hanya penerima yang dituju yang dapat memperoleh isi pesan. Alice ingin hanya Bob yang menerima pesannya, bukan Eve, baik Eve menguping dari bawah cucuran atap maupun mencegat pesan ketika pesan tersebut bergerak dalam suatu bentuk dari Alice menuju Bob.

DEFINISI 4.1.2. **Integritas** pesan berarti penerima dapat memastikan bahwa pesan tersebut tidak diubah. Bob ingin mengetahui bahwa yang diterimanya adalah apa yang ditulis Alice, bukan hasil perubahan yang dikehendaki Eve yang usil.

DEFINISI 4.1.3. **Autentikasi** pengirim berarti penerima dapat menentukan identitas pengirim dari pesan tersebut. Bob ingin memastikan bahwa pesan itu benar-benar berasal dari Alice.

[1]Kata Inggris *eavesdropper* konon berasal dari kata Inggris Kuno *yfesdrype*, yang secara harfiah berarti seseorang yang berdiri di *eavesdrop* [tanah tempat air menetes dari cucuran atap] untuk mendengarkan percakapan di dalam rumah.

DEFINISI 4.1.4. **Nirpenyangkalan** pengirim berarti pengirim tidak dapat menyangkal bahwa ia telah mengirim pesan tersebut. Bob ingin dapat menuntut Alice menepati janji yang dinyatakannya.

Perhatikan bahwa Alice dan Bob sebenarnya dapat merupakan orang yang sama, yang mengirim pesan dari dirinya pada masa lalu kepada dirinya pada masa depan. Misalnya, seseorang mungkin ingin menyimpan catatan yang harus tetap *rahasia* dan dapat diandalkan *integritasnya*, bahkan jika tempat penyimpanan catatan tersebut dibobol.

Salah satu skema paling awal yang berusaha mencapai kerahasiaan mungkin digunakan sekitar abad ke-7 SM di Yunani. Para panglima militer ingin menerima laporan dari prajurit yang berada jauh dan mengirimkan perintah kepada mereka sedemikian rupa sehingga, sekalipun pembawa pesan tertangkap, pesan yang dibawanya tidak dapat dibaca musuh. Mereka menggunakan alat bernama **scytale** (dalam pelafalan Inggris, huruf "c" dibaca keras dan katanya berima dengan "Italy"). Alat ini berupa tongkat silindris—mungkin batang tombak—($\sigma\kappa\upsilon\tau\acute{\alpha}\lambda\eta$ berarti *tongkat* dalam bahasa Yunani Kuno), yang dililit secara spiral dengan selembar perkamen panjang. Pesan kemudian dapat ditulis dalam baris-baris sejajar *sepanjang scytale*. Ketika lembaran itu dilepas, semua hurufnya menjadi teracak dan pesannya tidak dapat dibaca.

GAMBAR 4.1.1. Sebuah scytale sedang digunakan.[2]

Di tempat tujuan, dengan asumsi penerima juga mempunyai scytale, pesan akan muncul kembali seolah-olah secara ajaib ketika lembaran itu dililitkan secara spiral dan dibaca memanjang.

Sebelum melanjutkan, kita memerlukan beberapa istilah teknis lagi.

[2]Gambar oleh DMGualtieri, CC BY-SA 3.0 http://creativecommons.org/licenses/by-sa/3.0, melalui Wikimedia Commons, diunduh dari https://commons.wikimedia.org/wiki/File%3AScytale.png

DEFINISI 4.1.5. Pesan yang hendak dikirim Alice kepada Bob dalam bentuk aslinya (dan bentuk akhir yang dipulihkan) disebut **plainteks** atau **teks terang**.

DEFINISI 4.1.6. Algoritme yang digunakan Alice untuk mengubah (mengaburkan) plainteks menjadi bentuk yang tetap rahasia sekalipun diamati Eve selama pengiriman disebut **cipher** atau algoritme sandi. Kita juga mengatakan bahwa Alice **mengenkripsi** pesan (plainteks) tersebut.

DEFINISI 4.1.7. Setelah dienkripsi, pesan tersebut disebut **cipherteks** atau **teks sandi**.

DEFINISI 4.1.8. Ketika menerima cipherteks, Bob menerapkan algoritme lain untuk **mendekripsinya** dan memulihkan plainteks.

Secara grafis:

Istilah dasar kripto:

Alice	pada jaringan publik	Bob
plainteks/teks terang pesan m **mengenkripsi** m menjadi c mengirim c	$\rightarrowtail$ **cipherteks** c $\rightarrowtail$	menerima c **mendekripsi** c untuk memulihkan plainteks m

Andaikan seorang mata-mata melihat para pengintai di lapangan melilitkan lembaran perkamen pada tombak dan menulis sepanjang tombak itu. Artinya, Eve mengetahui algoritme enkripsinya. Meskipun *algoritmenya* diketahui, kerahasiaan masih mungkin dipertahankan.

DEFINISI 4.1.9. Informasi tambahan—sebagian digunakan dalam enkripsi dan sebagian diperlukan agar dekripsi berhasil—disebut **kunci**.

Dalam enkripsi menggunakan scytale, diameter scytale merupakan kuncinya. Bahkan, ada dugaan bahwa scytale juga berfungsi sebagai bentuk autentikasi sederhana: hanya Alice yang mempunyai scytale yang cocok dengan milik Bob. Jadi, jika Bob dapat membaca rangkaian huruf yang bermakna di sepanjang scytale miliknya, ia mengetahui bahwa Alicelah yang mengirimkannya.

Bahkan dengan kunci, kelemahan kriptosistem ini cukup jelas. Dan Athena memang kalah dalam Perang Peloponnesos.

Pengalaman kriptologi selama berabad-abad menunjukkan bahwa algoritme suatu kriptosistem justru sebaiknya dibuka kepada publik, sedangkan hanya kunci bagi saluran komunikasi tertentu (misalnya antara Alice dan Bob) yang dirahasiakan. Ada banyak alasan untuk pendekatan ini. Alasan utamanya barangkali adalah bahwa pembuat kriptosistem tidak pernah dapat memastikan bahwa ia telah memikirkan semua metode kriptanalisis yang mungkin digunakan untuk menyerang sistemnya. Karena itu, lebih baik pembuat sistem membiarkan komunitas kripto seluas-luasnya menguji sistem tersebut, dan hanya sistem yang telah bertahan terhadap serangan semacam itu yang patut digunakan. Bagaimanapun, inilah dasar metode ilmiah: ilmuwan menerbitkan seluruh rincian eksperimennya agar orang lain dapat mencobanya, memberikan verifikasi independen, atau menemukan sesuatu yang perlu dikritik.

Gagasan bahwa keamanan kriptosistem harus bertumpu pada kerahasiaan kunci, bukan kerahasiaan algoritme, dikenal sebagai **Prinsip Kerckhoffs** . Nama itu merujuk pada gagasan perancangan kriptosistem yang ditulis Auguste Kerckhoffs pada tahun 1883 dalam karya

dua bagiannya, *La Cryptographie militaire*. Prinsip ini berlawanan dengan kriptosistem yang dianggap sangat lemah karena bergantung pada harapan bahwa algoritmenya tidak akan pernah diketahui. Sistem semacam itu bertumpu pada paradigma **keamanan melalui ketertutupan** (*security through obscurity*) yang tidak bijaksana.

Latihan untuk §4.1.

LATIHAN 4.1.1. Andaikan, untuk suatu $k \in \mathbb{N}$, plainteks yang hendak dikirim Alice terdiri atas simbol-simbol $m_1, \ldots, m_k$. Andaikan diameter scytale yang digunakannya memungkinkan $s \in \mathbb{N}$ huruf ditulis pada setiap putaran spiral perkamen ketika perkamen itu dililitkan pada scytale.

Tuliskan satu atau beberapa rumus yang mendeskripsikan huruf-huruf $c_1, \ldots, c_k$ dalam cipherteks. Anda harus mengandaikan $s < k$ dan, jika diinginkan, boleh mengandaikan hubungan tertentu yang berguna, seperti $s \mid k$.

LATIHAN 4.1.2. Sekalipun kriptosistem scytale kuat, penggunaannya untuk *autentikasi* mungkin bermasalah. Jelaskan bagaimana autentikasi dapat gagal bergantung pada pesan yang dikirim; berikan satu atau dua contoh pesan yang "buruk" untuk autentikasi.

LATIHAN 4.1.3. Kriptosistem scytale tampak lemah. Jelaskan bagaimana Anda akan melakukan kriptanalisis terhadapnya.

4.2. Cipher Caesar dan Varian-Variannya

Sistem lain yang berasal dari zaman kuno konon digunakan oleh Julius Caesar.

DEFINISI 4.2.1. Alice mengambil pesannya, menghapus semua spasi dan tanda baca, lalu menyamakan kapitalisasi seluruh hurufnya (misalnya menjadi huruf kapital). Kemudian ia menggeser setiap huruf sejauh k posisi ke depan dalam alfabet, kembali dari Z ke A jika perlu. Di sini $k \in \mathbb{Z}$ adalah bilangan tetap yang hanya diketahui Alice dan Bob serta disebut **kunci**.

Untuk mendekripsi, Bob cukup menggeser setiap huruf sejauh k posisi ke belakang dalam alfabet, kembali dari A ke Z jika perlu. Dengan kata lain, Bob mengenkripsi cipherteks menggunakan kunci $-k$ untuk memperoleh plainteks.

Sistem ini disebut **kriptosistem Caesar**.

Julius Caesar tampaknya biasa menggunakan nilai kunci $k = 3$. Octavian, cucu dari saudari Julius Caesar, kemudian menjadi Kaisar Augustus dan suka menggunakan $k = -1$.

Jika kita menggunakan apa yang disebut alfabet Latin (meskipun alfabet ini bukan alfabet yang digunakan di Romawi kuno) dengan 26 huruf, ada satu nilai kunci yang sangat menarik: 13. Dengan nilai itu, enkripsi dan dekripsi merupakan transformasi yang persis sama. Pada zaman modern, transformasi ini disebut **ROT13**, dan pernah memainkan peran kecil dalam sejarah modern Internet. Misalnya, kiriman di ruang obrolan dan papan buletin awal kadang-kadang memuat bagian yang tidak boleh langsung terlihat oleh siapa saja yang membaca kiriman, tetapi tetap dapat dibuka oleh pembaca yang bersungguh-sungguh (seperti bocoran alur dalam ulasan gim, buku, atau film baru yang populer). Bagian semacam itu sering disertakan setelah terlebih dahulu diproses dengan ROT13.

Walaupun sebenarnya sama sekali tidak aman, ROT13 bahkan pernah digunakan untuk tujuan keamanan yang sesungguhnya dalam beberapa produk komersial, termasuk pada bagian tertentu dari beberapa versi sistem operasi Windows.

Cipher Caesar sudah berhasil dipecahkan sepenuhnya (dengan beberapa cara; lihat §4.3 di bawah) sebelum tahun 1000 M, tetapi salah satu turunannya dikembangkan pada akhir Abad Pertengahan dan dianggap sebagai teknologi kriptologi termaju hingga awal zaman modern.

DEFINISI 4.2.2. Sekali lagi, Alice mengambil pesannya, menghapus semua spasi dan tanda baca, lalu menyamakan kapitalisasi seluruh hurufnya (misalnya menjadi huruf kapital). Kali ini, kunci $\vec{k} = (k_1, \ldots, k_\ell)$ yang dimiliki bersama oleh Alice dan Bob merupakan tupel-ℓ, untuk $\ell \in \mathbb{N}$, yang terdiri atas bilangan bulat $k_1, \ldots, k_\ell \in \mathbb{Z}$.

Untuk mengenkripsi, Alice menelusuri pesan plainteks dan barisan kuncinya bersama-sama, satu huruf demi satu huruf. Setiap huruf plainteks digeser ke depan (kembali dari Z

ke A jika perlu) sebanyak bilangan yang ditentukan oleh komponen kunci yang bersesuaian. Jika komponen kuncinya habis, Alice kembali ke awal barisan kunci.

Untuk mendekripsi, Bob menggeser setiap huruf ke belakang sesuai komponen kunci yang bersesuaian, kembali dari A ke Z jika perlu. Dengan kata lain, Bob mengenkripsi menggunakan kunci $-\vec{k} = (-k_1, \ldots, -k_\ell)$.

Sistem ini disebut **kriptosistem Vigenère**.

Secara tradisional, kunci Vigenère berupa sebuah kata yang dituliskan, dihafalkan, dan dimiliki bersama oleh Alice dan Bob. Ketika mengenkripsi atau mendekripsi, huruf-huruf kata kunci itu "ditambahkan" pada huruf-huruf pesan seperti dijelaskan di atas, dengan konvensi $A = 1$, $B = 2$, dan seterusnya.

Perhatikan bahwa Vigenère dengan panjang kunci ℓ pada dasarnya merupakan ℓ cipher Caesar yang berjalan paralel. Bahkan, jika $\ell = 1$, keduanya merupakan kriptosistem yang persis sama. Karena itu, Vigenère pada dasarnya $\ell + 1$ kali lebih sulit dipecahkan daripada Caesar; suku "$+ 1$" muncul karena Eve bahkan tidak mengetahui ℓ. Meskipun demikian, setelah beberapa ratus tahun dianggap tidak dapat dipecahkan dan digunakan sebagai cipher diplomatik utama di istana-istana Eropa, metode untuk memecahkan Vigenère akhirnya dikembangkan.

Sebagai varian terakhir cipher Vigenère, andaikan kita bergerak ke arah yang berlawanan dari kasus ekstrem $\ell = 1$ dan memilih ℓ sepanjang mungkin.

DEFINISI 4.2.3. **Pad sekali pakai** (*one-time pad*) adalah kriptosistem Vigenère yang kuncinya sama panjang dengan pesan, dipilih secara acak, dan tidak pernah digunakan kembali. [Kunci dalam kriptosistem ini juga disebut *pad sekali pakai*[3].]

(Pad sekali pakai kadang-kadang disebut *Cipher Vernam* . Sebutan ini tidak tepat jika dilihat dari sejarah intelektual kriptosistem yang sebenarnya.)

Barisan kunci yang baik sangat penting dalam kriptosistem pad sekali pakai. Kabar baiknya, dapat dibuktikan bahwa jika pad sekali pakai benar-benar acak, kriptosistem yang dihasilkan memang aman secara sempurna. Dalam ilmu komputer, sifat ini disebut *aman secara teori informasi* , sebab bukti keamanannya tidak bergantung pada asumsi apa pun tentang sumber daya komputasi yang tersedia bagi penyerang. [Lihat [**Sha49**] dan [**Sha48**] untuk bukti tersebut.] Kriptosistem lain yang akan kita jumpai di bawah hanya aman jika kita mengandaikan bahwa penyerang mempunyai akses ke komputer jenis tertentu (asumsi yang lazim ialah sebuah *mesin Turing waktu-polinomial probabilistik*; bidang ilmu komputer yang membahas hal ini disebut *kompleksitas komputasi*; lihat, misalnya, [**AB09**]).

[3]Sinekdoke lagi!

Pad yang sama juga tidak boleh digunakan lebih dari sekali. Jika digunakan kembali, penyerang dapat mengambil selisih kedua cipherteks huruf demi huruf, yang akan meniadakan pad sepenuhnya dari perhitungan. Setelah itu, pesan biasanya dapat ditentukan dengan cepat.

Pada zaman modern, setelah munculnya jaringan komunikasi digital, pesan ditulis sebagai data komputer. Dengan demikian, semuanya disimpan (dan dikirimkan) sebagai bit, yaitu 1 dan 0. Untuk bit, padanan penggeseran huruf dalam alfabet dengan kembali dari Z ke A bila perlu adalah: tidak melakukan apa pun jika besar pergeserannya genap, atau menukar 0 dan 1 jika pergeserannya ganjil.

Dengan kata lain, jika pesan dan kunci sama-sama dituliskan seluruhnya sebagai bit—anggap setiap bit sebagai salah satu dari elemen $[0], [1] \in \mathbb{Z}/2\mathbb{Z}$—enkripsi tepat berupa penjumlahan bit-bit yang bersesuaian modulo 2. Karena itu, pad sekali pakai yang baik merupakan untaian bit (kelas-kelas kongruensi dalam $\mathbb{Z}/2\mathbb{Z}$) yang sangat acak dan sangat panjang.

Masalah besar pad sekali pakai adalah *distribusi kunci:* Alice dan Bob harus sudah memiliki bersama pad sekali pakai yang sangat besar sebelum mulai berkomunikasi. Panjangnya harus sekurang-kurangnya sama dengan jumlah seluruh huruf (atau bit pada zaman komputer) dalam semua pesan yang akan mereka kirim pada masa depan.

Hal ini menyarankan pendekatan menarik terhadap kriptografi: carilah cara agar Alice dan Bob dapat berbagi sebuah rahasia kecil yang memungkinkan keduanya menghasilkan barisan bit sepanjang apa pun, memperoleh barisan yang sama, tetapi barisan itu tampak sepenuhnya acak bagi setiap penyerang. Jika hal ini mungkin, mereka dapat menggunakan barisan *acak semu* tersebut sebagai pad sekali pakai. Disebut acak semu karena barisan itu sebenarnya tidak acak—Alice dan Bob dapat menentukannya terlebih dahulu dari rahasia awal yang kecil—tetapi bagi semua penyerang barisan itu tampak acak. [Lihat [**Lub96**] untuk pembahasan lebih lanjut tentang keacakan semu.]

Latihan untuk §4.2.

LATIHAN 4.2.1. ROT13 dianggap menarik karena mengurangi banyaknya kode yang perlu dibuat: program yang sama dapat melakukan dekripsi maupun enkripsi, sebab penerapan ROT13 untuk kedua kalinya membatalkan transformasi ROT13 yang pertama.

Apakah hal yang sama berlaku untuk cipher Caesar berkunci lainnya? Buatlah konjektur tentang apakah, untuk suatu kunci cipher Caesar $k \in \mathbb{Z}$ dan pesan m, selalu terdapat $n \in \mathbb{N}$ sedemikian sehingga

$$\overbrace{e_k^C \circ \cdots \circ e_k^C}^{n \text{ kali}}(m) = m$$

di mana e_k^C adalah fungsi enkripsi Caesar dengan kunci k. Jika ya, carilah rumus untuk n terkecil semacam itu, yang boleh bergantung (jika perlu) pada k, m, dan banyaknya huruf dalam alfabet yang digunakan untuk menulis m.

LATIHAN 4.2.2. Lanjutkan latihan sebelumnya. Sekarang andaikan $\vec{k} = (k_1, \ldots, k_\ell)$ merupakan tupel-ℓ, untuk $\ell \in \mathbb{N}$, yang terdiri atas bilangan bulat $k_1, \ldots, k_\ell \in \mathbb{Z}$, dan $e_{\vec{k}}^V$ adalah fungsi enkripsi Vigenère dengan kunci $\vec{k}$. Tentukan apakah, untuk setiap pesan m, terdapat $n \in \mathbb{N}$ sedemikian sehingga

$$\overbrace{e_{\vec{k}}^V \circ \cdots \circ e_{\vec{k}}^V}^{n \text{ kali}}(m) = m$$

dan, jika ya, carilah rumus untuk n terkecil semacam itu, yang boleh bergantung (jika perlu) pada $\vec{k}$, m, dan banyaknya huruf dalam alfabet yang digunakan untuk menulis m.

LATIHAN 4.2.3. Andaikan Eve mempunyai kembaran bernama Vev. Keduanya mengamati cipherteks c yang dikirim Alice kepada Bob dan berhasil mereka cegat. Mereka menduga bahwa pasangan kekasih konyol Alice dan Bob menggunakan pad sekali pakai untuk mengenkripsi komunikasi mereka. Eve dan Vev sama-sama melakukan banyak perhitungan dan mengira telah berhasil mendekripsi c dengan benar. Sayangnya, Eve dan Vev masing-masing memperoleh nilai m_e dan m_v yang berbeda (dan keduanya bermakna!), lalu menganggap nilainya sebagai plainteks yang hendak dikirim Alice kepada Bob.

Pad sekali pakai p_e dan p_v apakah yang, menurut perhitungan (atau tebakan) mereka masing-masing, digunakan Alice?

Apakah hasil dekripsi usulan m_e dan m_v dapat dipilih sembarang, atau adakah hubungan antara kedua hasil dekripsi usulan, pad usulan p_e dan p_v, plainteks sebenarnya, serta pad sekali pakai yang benar-benar digunakan Alice?

Kerjakan satu contoh konkret. Jika pesan teks terang asli Alice m adalah `aardvark`, mungkinkah Eve mengira pesannya $m_e =$ `iloveyou`, sedangkan Vev mengira pesannya $m_v =$ `ihateyou`? Jika mungkin, berikan contoh cipherteks c yang bersesuaian, pad sekali pakai Alice dan Bob p_{AB}, hasil dekripsi usulan m_e dan m_v, serta pad sekali pakai usulan p_e dan p_v.

4.3. Langkah Awal dalam Kriptanalisis: Analisis Frekuensi

Cipher Caesar tampak sangat lemah. Namun, ketika kita melihat suatu cipherteks, seperti

```
wrehruqrwwrehwkdwlvwkhtxhvwlrq
zkhwkhuwlvqreohulqwkhplqgwrvxiihu
wkhvolqjvdqgduurzvrirxwudjhrxviruwxqh
ruwrwdnhdupvdjdlqvwdvhdriwurxeohv
dqgebrssrvlqjhqgwkhp
```

sulit untuk mengetahui harus mulai dari mana—teks itu nyaris sama sekali tidak tampak seperti bahasa Inggris.

Mungkin kita perlu mulai dari cipher Caesar itu sendiri, dengan mengandaikan (secara anakronistis) bahwa Caesar mengikuti Prinsip Kerckhoffs, atau (lebih sesuai dengan zamannya) bahwa para mata-mata telah mengetahui kriptosistemnya tetapi belum mengetahui kuncinya.

Kita segera menyadari bahwa hal yang tidak diketahui, yaitu kunci, begitu kecil dibandingkan dengan kesulitan yang ditimbulkannya. Bahkan, jika kita memilih kunci secara acak, hampir empat dari 100 percobaan akan menghasilkan dekripsi yang benar semata-mata karena keberuntungan. Perhitungan ini menggunakan "alfabet Latin" modern yang terdiri atas 26 huruf; pada zaman Caesar, alfabet Latin yang sebenarnya hanya memiliki 23 huruf, sehingga peluangnya bahkan lebih baik. Secara formal, kita membicarakan konsep berikut.

DEFINISI 4.3.1. Himpunan semua kunci yang sah untuk suatu kriptosistem disebut **ruang kunci**.

CONTOH 4.3.2. Ruang kunci kriptosistem cipher Caesar adalah alfabetnya.

CONTOH 4.3.3. Ruang kunci kriptosistem cipher Vigenère dengan panjang kunci ℓ adalah semua barisan yang terdiri atas ℓ huruf dalam alfabet. Karena itu, ruang tersebut memiliki N^ℓ elemen jika alfabetnya berukuran N. Jika panjang kunci yang tepat tidak diketahui, tetapi diketahui tidak melebihi suatu batas $L \in \mathbb{N}$, terdapat $\sum_{j=1}^{L} N^j$ kemungkinan kunci.

CONTOH 4.3.4. Setiap barisan huruf sepanjang M merupakan kemungkinan kunci (pad) untuk enkripsi pad sekali pakai atas pesan sepanjang M. Karena itu, terdapat N^M kemungkinan pad sekali pakai untuk pesan sepanjang M pada alfabet berukuran N.

Kita menghitung ukuran berbagai ruang kunci tersebut karena salah satu kelemahan cipher Caesar adalah ruang kuncinya yang begitu kecil. Strategi yang lebih baik daripada menebak secara acak ialah mencoba semua kunci yang mungkin dan melihat kunci mana yang menghasilkan dekripsi yang benar. Hanya ada 26 kunci (atau 23 pada zaman Julius)!

Pendekatan ini disebut *serangan brute force* [atau *pencarian menyeluruh*]. Bahkan pada zaman Caesar, ruang kunci cipher Caesar sudah begitu kecil sehingga Eve dapat memeriksa semua kunci dan melihat kunci mana yang menghasilkan teks terang pesan Alice kepada Bob.

Cipher Vigenère sedikit lebih sulit. Sebagai contoh, jika panjang kunci diketahui sama dengan lima, hampir 12 juta kunci harus dicoba. Sebelum zaman komputer, pekerjaan ini sama sekali tidak mungkin ditangani. Bahkan pada abad ke-21, ketika komputer dapat menghasilkan semua kemungkinan dekripsi itu dalam waktu yang bagi manusia tampak seketika, masih ada masalah: manusia harus memeriksa 12 juta kemungkinan tersebut dan memilih dekripsi yang sah.

Mechanical Turk milik Amazon (lihat `https://www.mturk.com/mturk/welcome`) mungkin dapat menghimpun cukup banyak tenaga manusia untuk menyelesaikan satu dekripsi Vigenère dengan brute force. Namun, pendekatan yang lebih baik ialah menulis program komputer yang dapat membedakan teks tanpa makna dari pesan nyata yang mungkin dikirim Alice kepada Bob. Dengan begitu, serangan brute force dapat berhasil dalam beberapa saat.

Untuk membedakan teks tanpa makna dari pesan nyata, kita perlu mengetahui pesan-pesan nyata apa saja yang mungkin. Hal ini memotivasi definisi berikut.

DEFINISI 4.3.5. Himpunan pesan yang mungkin dalam suatu komunikasi terenkripsi disebut **ruang pesan**.

Tanpa suatu struktur pada ruang pesan, kriptanalisis dapat menjadi nyaris mustahil. Misalnya, jika Alice mengirimkan kode kombinasi sebuah brankas kepada Bob melalui surel dalam bentuk terenkripsi, ruang pesannya tidak terlalu besar tetapi tidak mempunyai ciri yang dapat dikenali. Serangan brute force tidak memiliki cara untuk menentukan hasil dekripsi mana yang merupakan kode kombinasi sebenarnya.

Namun, andaikan ruang pesan komunikasi Alice dan Bob berupa himpunan teks pendek (atau panjang, yang lebih baik) dalam bahasa Inggris. Teks bahasa Inggris mempunyai cukup banyak struktur; manusia penutur bahasa Inggris tentu dapat mengenali bahasa Inggris yang wajar. Pertanyaannya ialah apakah proses mendeteksi teks bahasa Inggris yang wajar dapat diotomatisasi.

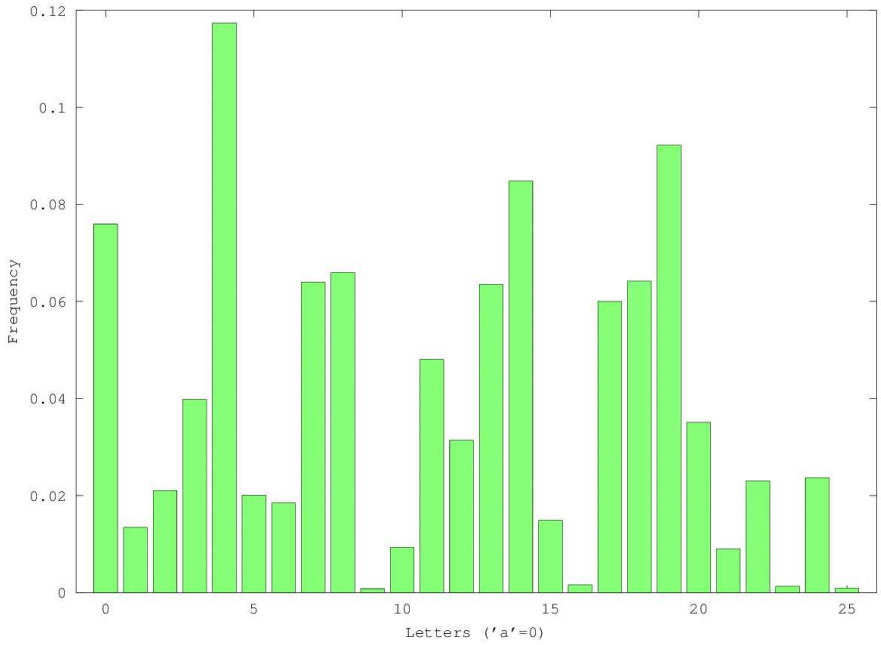
Mari kita lihat kembali contoh enkripsi Caesar pada awal bagian ini. Kita sudah melihat bahwa hasilnya tidak tampak seperti bahasa Inggris—tetapi dalam hal apa? Salah satunya tentu karena teks itu tidak memuat kata bahasa Inggris. Orang yang mengetahui bahasa Inggris mengenal sebagian besar kosakatanya dan dapat melihat bahwa teks tersebut tidak memuat kata-kata itu, kecuali mungkin “up” dan “i” (beberapa kali).

Hal ini menyarankan sebuah pendekatan: ambil daftar semua kata bahasa Inggris beserta semua bentuk varian dan turunannya; tambahkan beberapa barisan acak pendek yang mungkin muncul di dalam bahasa Inggris baku (misalnya ketika Alice mengutip ucapan

tanpa makna yang didengarnya atau menyalin grafiti pada sisi gerbong kereta bawah tanah); lalu bandingkan daftar itu dengan semua kemungkinan dekripsi cipherteks. Skema ini tidak terlalu praktis. Namun, jika ruang pesannya cukup kecil, pendekatan semacam ini masuk akal.

Jika kita kembali melihat pesan tersebut, pembaca bahasa Inggris juga segera merasa bahwa huruf atau kombinasi hurufnya tidak tepat. Misalnya, tampaknya tidak ada cukup banyak vokal. Pemeriksaan seberapa sering huruf muncul dalam sebuah teks dibandingkan dengan frekuensi yang diharapkan disebut *analisis frekuensi*. Penggunaannya dalam kriptanalisis tampaknya pertama kali dijelaskan oleh filsuf dan matematikawan Muslim al-Kindi [4] dalam karyanya pada abad ke-9, *Manuskrip tentang Penguraian Pesan Kriptografis*.

Berikut adalah tabel frekuensi huruf dalam sejumlah teks bahasa Inggris baku (beberapa drama Shakespeare):



GAMBAR 4.3.1. Frekuensi huruf dalam beberapa drama Shakespeare

Perhatikan bahwa huruf ‘e’ merupakan huruf yang paling sering muncul, meskipun hanya dengan selisih kecil. Jadi, pendekatan kriptanalisis pertama menggunakan analisis frekuensi dapat dilakukan dengan memilih kunci dekripsi Caesar yang menggeser huruf paling sering dalam cipherteks menjadi ‘e’. Untuk cipherteks pada awal bagian ini, pendekatan tersebut menghasilkan dekripsi:

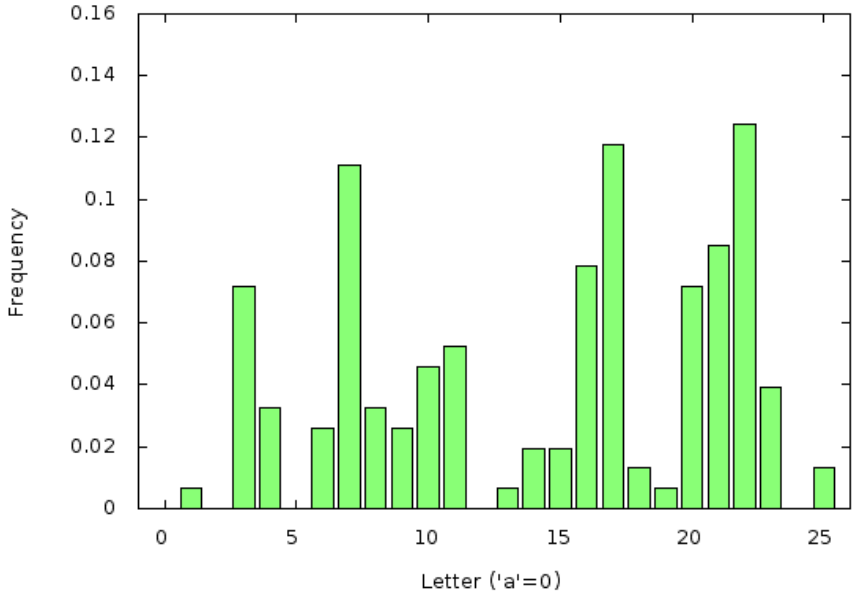
```
ezmpzcyzeezmpesletdespbfpdetzy
hspespcetdyzmwpctyespxtyoezdfqqpc
```

[4] Al-Kindi adalah tokoh yang sangat menarik dalam sejarah intelektual Muslim awal. Sebagai contoh, tampaknya ia memperkenalkan bilangan Hindu beserta notasi nilai tempatnya ke dunia Muslim.

```
espdwtyrdlyolcczhdzqzfeclrpzfdqzcefyp
zcezelvplcxdlrltydeldplzqeczfmwpd
lyomjzaazdtyrpyoespx
```

Hasilnya kurang baik. Rupanya, hanya memperhatikan huruf yang paling sering belum cukup: huruf paling sering dalam plainteks pesan ini bukan ‘e’.

Sebagai gantinya, mari kita lihat seluruh tabel frekuensi cipherteks ini.



GAMBAR 4.3.2. Frekuensi huruf dalam contoh cipherteks Caesar

Sayangnya, hasil ini tidak persis sama dengan distribusi frekuensi bahasa Inggris baku (berdasarkan Shakespeare), bahkan bukan sekadar versi distribusi Shakespeare yang digeser (dengan kembali dari 25 ke 0). Namun, mungkin salah satu pergeserannya cukup dekat dengan distribusi Shakespeare.

Hal ini menyarankan pendekatan kriptanalisis yang lebih halus: coba semua kemungkinan dekripsi (tidak terlalu berat untuk cipher Caesar karena ruang kuncinya kecil), lalu pilih hasil yang seluruh tabel frekuensi hurufnya paling dekat dengan tabel frekuensi bahasa Inggris baku. Jadi, kita *tidak* hanya melihat huruf yang paling sering, melainkan seluruh distribusi frekuensinya; dan kita *tidak* mencari kecocokan persis, melainkan kecocokan hampiran terbaik.

Pertanyaan berikutnya ialah cara terbaik untuk mengukur jarak antara dua distribusi. Salah satu pendekatan yang lazim ialah mengukur besaran berikut.

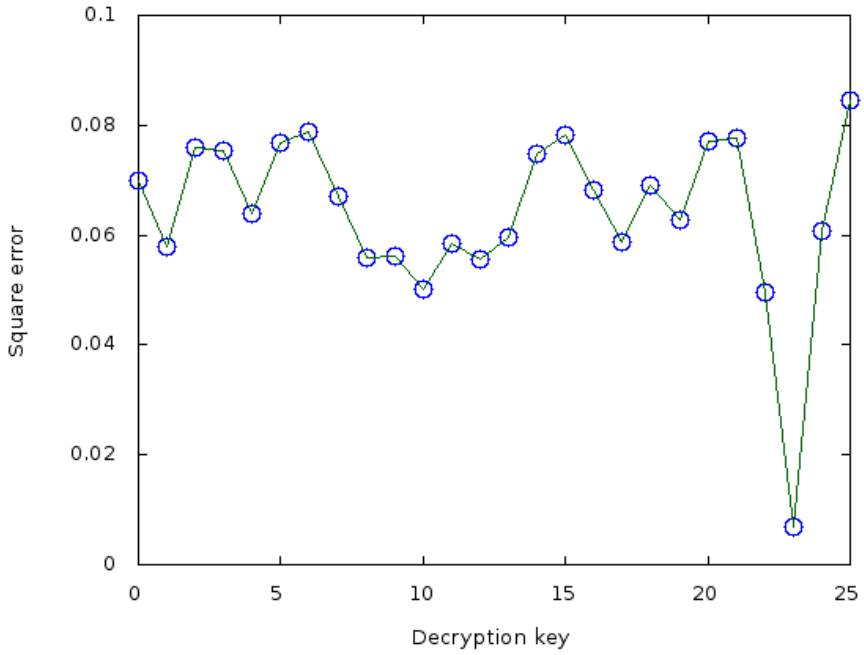
DEFINISI 4.3.6. **Galat kuadrat total** adalah jarak antara dua distribusi f dan g yang diberikan oleh

$$d(f,g) = \sum_{j=0}^{25} (f(j) - g(j))^2$$

di mana distribusi selalu didefinisikan pada huruf dalam bentuk 'a'=0, 'b'=1, dan seterusnya.

Meminimumkan jarak ini ekuivalen dengan metode *kuadrat terkecil* dalam statistika atau aljabar linear.

Dengan menerapkan strategi ini pada cipherteks dari awal bagian, kita memperoleh hasil berikut.



GAMBAR 4.3.3. Galat kuadrat untuk semua kunci dekripsi pada contoh cipherteks Caesar

Galat kuadrat minimum diperoleh dari kunci dekripsi 23 (yang bersesuaian dengan kunci enkripsi awal 3; secara anakronistis, enkripsi ini dilakukan oleh Julius sendiri). Teks terang yang bersesuaian adalah

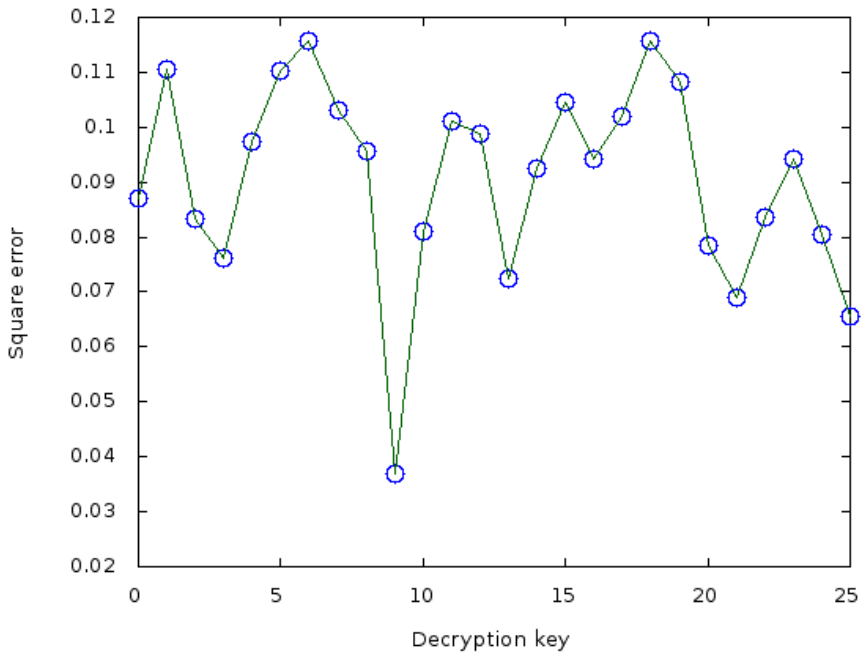
```
tobeornottobethatisthequestion
whethertisnoblerinthemindtosuffer
theslingsandarrowsofoutrageousfortune
ortotakearmsagainstaseaoftroubles
andbyopposingendthem
```

yang tampak cukup meyakinkan.

Menariknya, pendekatan untuk mendeteksi teks bermakna ini cukup tangguh, bahkan untuk teks sangat pendek yang distribusi frekuensinya mungkin cukup jauh dari standar bahasa Inggris. Sebagai contoh, untuk cipherteks

```
rkkrtbrkeffespkyvtifjjifruj
```

kita memperoleh



GAMBAR 4.3.4. Galat kuadrat untuk semua kunci dekripsi pada cipherteks Caesar `rkkrtbrkeffespkyvtifjjifruj`

yang menunjukkan bahwa kunci dekripsinya adalah 9 dan bersesuaian dengan kunci enkripsi 17. Jadi, teks terangnya pasti

```
attackatnoonbythecrossroads
```

yang tampak seperti sesuatu yang mungkin dikatakan Julius.

Cukup sampai di sini kriptanalisis cipher Caesar. Ketika beralih ke Vigenère, persoalan pertama adalah menentukan panjang kunci. Jika panjang kunci ℓ diketahui, kita dapat membagi cipherteks menjadi ℓ teks yang lebih pendek: teks pertama memuat karakter-karakter berselang ℓ posisi mulai dari karakter pertama, teks kedua mulai dari karakter kedua, dan seterusnya, hingga teks yang dimulai dari karakter ke-ℓ. Dengan menerapkan pemecah Caesar otomatis yang dijelaskan di atas, kita memperoleh ℓ komponen kunci dan kemudian plainteksnya.

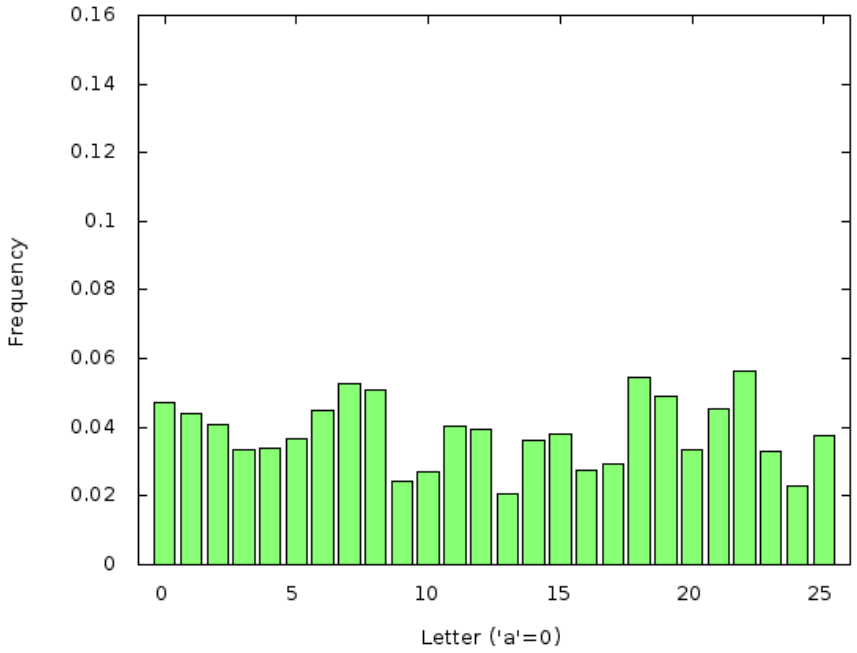
Untuk mempermudah, andaikan kita mengambil seluruh *Hamlet* dan mengenkripsinya dengan Vigenère menggunakan kata kunci `hippopotomonstrosesquipedaliophobia`, yang bersesuaian dengan kunci numerik

$$k = (7, 8, 15, 15, 14, 15, 14, 19, 14, 12, 14, 13, 18, 19, 17, 14,$$
$$18, 4, 18, 16, 20, 8, 15, 4, 3, 0, 11, 8, 14, 15, 7, 14, 1, 8, 0)$$

Sebagai contoh, bagian cipherteks yang bersesuaian dengan kutipan untuk memecahkan cipher Caesar di atas adalah

```
hdxajnioomjvdtfvstrqitmfozlxjj
kcmiosgpenjjbgxmcmtfzltmaudofpmwg
odsntxuuhwjywmrjpnieosoqlfbpjoqyyljia
cmbdaozawminabtdhrtyndlncugkflswh
vjrwgdwddoeicznymcyl
```

Jika Eve berharap teks ini hanya dienkripsi dengan Caesar, sehingga panjang kunci Vigenère adalah $\ell = 1$, ia akan memperoleh frekuensi huruf berikut.

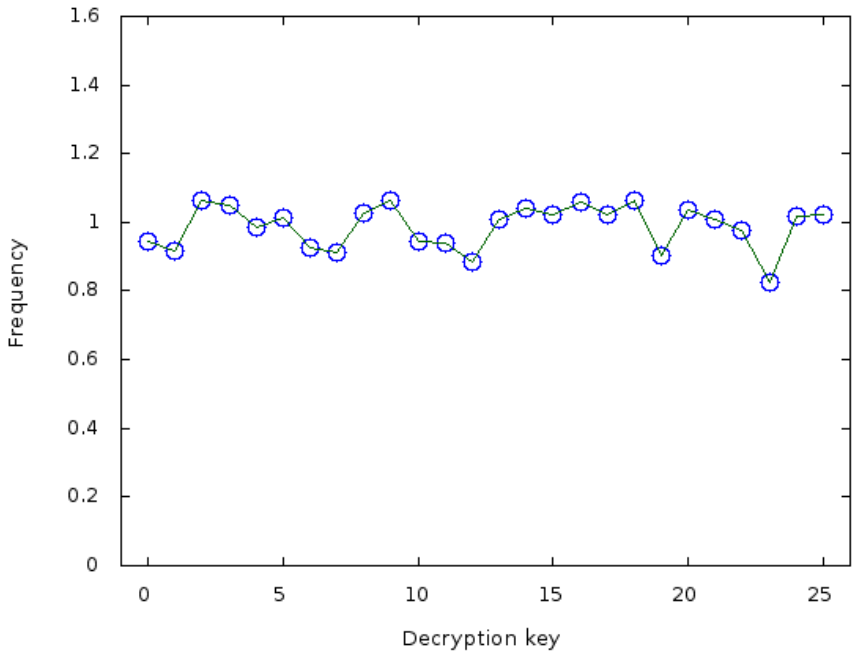


GAMBAR 4.3.5. Frekuensi huruf dalam enkripsi Vigenère atas *Hamlet* dengan kunci `hippopotomonstrosesquipedaliophobia`

Dibandingkan dengan Gambar 4.3.2, nilai-nilai ini menunjukkan variasi yang jauh lebih kecil. Bahkan, tidak ada nilai nol maupun nilai yang jauh lebih besar daripada semua nilai lainnya. Alasannya, secara hampiran distribusi ini merupakan campuran dari 35 pergeseran distribusi baku bahasa Inggris dalam Gambar 4.3.1, satu untuk setiap posisi kata kunci `hippopotomonstrosesquipedaliophobia`; jika pergeseran yang sama digabungkan, hasilnya adalah campuran berbobot dari 16 nilai pergeseran berbeda. Pencampuran ini menghaluskan seluruh bentuk khas distribusi yang berguna untuk mengenali pergeseran dekripsi yang benar.

Meskipun demikian, pemecah Caesar akan menghasilkan suatu nilai kunci untuk setiap kemungkinan nilai ℓ yang dicoba Eve. Untuk setiap posisi kunci, selalu ada nilai pergeseran yang meminimumkan galat kuadrat. Jika tebakan panjang kunci ℓ salah dan pengelompokan yang dihasilkan mencampurkan beberapa pergeseran berbeda, nilai minimum ini biasanya tidak terlalu kecil: distribusi frekuensi huruf pada posisi-posisi cipherteks yang kongruen dengan $k \pmod{\ell}$, untuk $k \in \mathbb{N}$ dan $k \leq \ell$, biasanya lebih datar, sehingga jauh (menurut jarak galat kuadrat) dari distribusi bahasa Inggris baku.

Sebagai contoh, pada enkripsi *Hamlet* yang sedang kita kaji, andaikan Eve menebak $\ell = 5$ dan mengambil semua huruf pada posisi yang kongruen dengan $1 \pmod 5$. Pemecah Caesar akan menghasilkan grafik galat kuadrat berikut:



GAMBAR 4.3.6. Galat kuadrat untuk semua kunci dekripsi pada huruf di posisi yang kongruen dengan $1 \pmod 5$ dalam *Hamlet* yang dienkripsi menggunakan Vigenère dengan kunci `hippopotomonstrosesquipedaliophobia`

Nilai minimum jelas terdapat pada kunci dekripsi 23, tetapi tidak jauh lebih kecil daripada kemungkinan lain. Selain itu, semua galatnya sekitar sepuluh kali lebih besar daripada yang tampak pada grafik sebelumnya, seperti Gambar 4.3.3.

Jadi, berikut adalah pendekatan kriptanalisis Vigenère. Coba semua panjang kunci ℓ hingga suatu batas L. Batas ini ditentukan oleh waktu komputasi yang tersedia dan tidak boleh begitu besar sehingga pengambilan huruf-huruf berselang ℓ posisi dari cipherteks menyisakan terlalu sedikit huruf untuk analisis frekuensi yang wajar. Untuk setiap ℓ anak untaian yang terdiri atas huruf-huruf berselang ℓ posisi dan masing-masing dimulai pada posisi $1, \ldots, \ell$, terapkan pemecah Caesar. Hasilnya adalah kunci Vigenère optimal $\vec{k}_\ell = (k_{\ell,1}, \ldots, k_{\ell,\ell})$ sepanjang ℓ. Kemudian, untuk setiap $\ell = 1, \ldots, L$ dan kunci $\vec{k}_\ell$ yang bersesuaian, hitung jarak galat kuadrat d_ℓ antara cipherteks yang didekripsi menggunakan $\vec{k}_\ell$ dan distribusi huruf bahasa Inggris baku. Laporkan ℓ dan $\vec{k}_\ell$ sebagai panjang kunci dan kunci Vigenère jika d_ℓ merupakan galat kuadrat terkecil yang diperoleh.

Latihan untuk §4.3.

LATIHAN 4.3.1. Dapatkah Anda menemukan cipherteks Caesar yang memiliki dua hasil dekripsi yang keduanya tampak seperti bahasa Inggris yang wajar selama serangan brute force? Jika dapat, berikan contoh yang tepat beserta kunci dekripsinya.

LATIHAN 4.3.2. Apakah latihan sebelumnya (4.3.1) menjadi lebih sulit atau lebih mudah untuk cipher Vigenère? Berikan alasan dan contoh.

LATIHAN 4.3.3. Dalam merancang kriptosistem yang aman, enkripsi yang lebih banyak tampaknya lebih baik. Jadi, bagaimana jika kita mengenkripsi teks terang dengan satu kriptosistem, lalu mengenkripsi kembali cipherteks yang dihasilkan untuk membuat sebuah cipherteks super?

Sejauh ini kita mempunyai dua kriptosistem berkunci pendek: Caesar dan Vigenère. Kita juga mempunyai pad sekali pakai, tetapi sistem itu sudah aman secara sempurna dan mempunyai kunci besar, yaitu pad-pad tersebut, sehingga tidak akan kita pertimbangkan. Andaikan saya membuat kriptosistem baru yang menerapkan suatu kombinasi enkripsi Caesar dan Vigenère secara berurutan, semuanya dengan kunci berbeda. Apakah hasilnya merupakan kriptosistem yang jauh lebih aman? Mengapa atau mengapa tidak?

4.4. Kripto Kunci Publik: Kriptosistem RSA

Andaikan Alice dan Bob tidak pernah berkesempatan bertemu langsung, tetapi tetap ingin bertukar pesan yang dirahasiakan dari Eve. Apa yang dapat mereka lakukan?

Hal ini tampak mustahil dalam konteks kriptosistem yang telah kita bahas. Mari kita uraikan bagian penting yang membuatnya begitu sulit.

DEFINISI 4.4.1. Sebuah **cipher simetris** (atau **kriptosistem simetris**) terdiri atas bagian-bagian berikut, yang semuanya diketahui oleh kedua pihak yang berkomunikasi dan juga oleh masyarakat umum:

- ruang pesan $\mathcal{M}$;
- ruang kunci $\mathcal{K}$;
- algoritme enkripsi yang menghasilkan cipherteks $c = e_k(m)$ untuk setiap pilihan $k \in \mathcal{K}$ dan $m \in \mathcal{M}$;
- algoritme dekripsi yang, jika diberi cipherteks c dan $k \in \mathcal{K}$, menghasilkan pesan $d_k(c) \in \mathcal{M}$ serta memenuhi $d_k(e_k(m)) = m \; \forall k \in \mathcal{K}, m \in \mathcal{M}$.

Alice dan Bob dapat menggunakan cipher simetris semacam ini dengan menyepakati secara privat sebuah kunci $k \in \mathcal{K}$ yang akan dipakai untuk enkripsi dan dekripsi. Karena itu, kriptosistem simetris juga disebut **kriptosistem kunci privat**.

Secara grafis:

Penyiapan dan notasi dasar kripto kunci privat:

komunikasi privat Alice $\longleftrightarrow$ pertukaran kunci bersama $k \in \mathcal{K}$ $\longleftrightarrow$ Bob		
	pada jaringan publik	
pesan $m_A \in \mathcal{M}$ hitung $c_A = e_k(m_A)$ kirim c_A	$\rightarrowtail$ cipherteks c_A $\rightarrowtail$	terima c_A hitung $m_A = d_k(c_A)$
terima c_B hitung $m_B = d_k(c_B)$	$\leftarrowtail$ cipherteks c_B $\leftarrowtail$	pesan $m_B \in \mathcal{M}$ hitung $c_B = e_k(m_B)$ kirim c_B
dan seterusnya		

Demi keamanan kriptosistem di atas, ruang kunci $\mathcal{K}$ harus cukup besar, atau keseluruhan sistem harus disusun sedemikian rupa sehingga sulit menentukan apakah suatu kemungkinan dekripsi tertentu sah (atau keduanya). Jika tidak, Eve dapat melakukan serangan brute force dengan mencoba semua kemungkinan kunci $k \in \mathcal{K}$ dan melihat hasil $d_k(c)$ mana yang masuk akal sebagai dekripsi.

Bagaimanapun, karena memerlukan pertukaran kunci privat di awal, kriptosistem simetris tidak cocok untuk situasi yang diajukan pada awal bagian ini. Kita memerlukan jenis kriptosistem yang berbeda.

DEFINISI 4.4.2. Sebuah **cipher asimetris** (atau **kriptosistem asimetris**) terdiri atas bagian-bagian berikut, yang semuanya diketahui oleh setiap pihak yang berkepentingan, baik yang sah maupun yang tidak:

- ruang pesan $\mathcal{M}$;
- ruang kunci enkripsi $\mathcal{K}_e$;
- ruang kunci dekripsi $\mathcal{K}_d$;
- algoritme pembangkitan kunci Gen yang menghasilkan pasangan terkait $(k_e, k_d) \in \mathcal{K}_e \times \mathcal{K}_d$;
- algoritme enkripsi yang menghasilkan cipherteks $c = e_{k_e}(m)$ untuk setiap pilihan $k_e \in \mathcal{K}_e$ dan $m \in \mathcal{M}$;
- algoritme dekripsi yang, jika diberi cipherteks c dan $k_d \in \mathcal{K}_d$, menghasilkan pesan $d_{k_d}(c) \in \mathcal{M}$ serta, untuk setiap pasangan (k_e, k_d) yang dihasilkan Gen, memenuhi $d_{k_d}(e_{k_e}(m)) = m \; \forall m \in \mathcal{M}$.

Untuk menggunakan kriptosistem semacam ini, Bob menjalankan Gen untuk memperoleh pasangan (k_e, k_d). Ia merahasiakan kunci dekripsi k_d, tetapi menyediakan kunci enkripsi k_e kepada publik (mungkin melalui situs webnya). Karena itu, k_e disebut **kunci publik** milik Bob dan k_d disebut **kunci privat** milik Bob, sedangkan keseluruhan sistem disebut **kriptosistem kunci publik**.

Secara grafis:

Penyiapan dan notasi dasar kripto kunci publik:

Alice	pada jaringan publik	Bob
		jalankan Gen untuk memperoleh $(k_e, k_d) \in \mathcal{K}_e \times \mathcal{K}_d$
unduh k_e	$\longleftarrow$ kunci publik k_e $\longleftarrow$	terbitkan k_e
pesan $m \in \mathcal{M}$ hitung $c = e_{k_e}(m)$ kirim c	$\longmapsto$ cipherteks c $\longmapsto$	terima c hitung $m = d_{k_d}(c)$

Seperti sebelumnya, keamanan kriptosistem ini terhadap serangan brute force bergantung pada ukuran $\mathcal{K}_d$. Selain itu, karena kunci dan algoritme enkripsi diketahui Eve, ruang pesan $\mathcal{M}$ tidak boleh terlalu kecil. Jika $\mathcal{M}$ kecil, Eve cukup menghitung semua enkripsi $e_{k_e}(m)$ untuk setiap $m \in \mathcal{M}$, lalu membandingkannya dengan cipherteks c yang berhasil dicegatnya.

Serangan terhadap ruang pesan ini dapat dicegah dengan memperbesar ruang tersebut secara artifisial. Biasanya, orang menambahkan data berikut.

DEFINISI 4.4.3. **Salt kriptografis** adalah data acak yang ditambahkan pada pesan yang hendak dikirim Alice kepada Bob sebelum dienkripsi, lalu dihapus secara otomatis di sisi Bob.

Setelah Alice menambahkan salt pada pesannya, Eve harus menelusuri seluruh ruang pesan beserta salt, yang dapat jauh lebih besar daripada $\mathcal{M}$.

Sebagai manfaat tambahan, salt membuat cipherteks hampir selalu berbeda pada setiap pengiriman rahasia, sekalipun plainteksnya sama, apabila dipilih secara independen dari ruang yang cukup besar. Eve tentu mengetahui bahwa Alice dan Bob sedang berkomunikasi, tetapi dengan hanya membandingkan kesamaan cipherteks, analisisnya tidak lagi dapat mengenali pengiriman ulang pesan yang sama secara andal. Tanpa salt, Eve yang cermat mungkin dapat menghubungkan cipherteks pesan dengan tindakan di dunia nyata, sehingga pada dasarnya mengetahui hasil dekripsinya tanpa memecahkan kriptosistem. Jika salt dipilih secara independen dari ruang yang cukup besar, korelasi yang hanya mengandalkan kesamaan cipherteks menjadi sangat tidak andal, sebab peluang penggunaan ulang salt yang sama menjadi sangat kecil.

Karena kunci enkripsi Bob k_e tersedia bagi publik, seluruh keamanan kriptosistem ini runtuh jika Eve dapat memulihkan kunci privat k_d yang bersesuaian. Di sisi lain, Bob harus dapat membangkitkan pasangan (k_e, k_d) secara layak pada tahap penyiapan. Asimetri antara komputasi maju yang mudah dan pemulihan rahasia yang sulit ini biasanya dibangun dari fungsi dengan sifat khusus berikut.

DEFINISI 4.4.4. Fungsi injektif $f : A \to B$ yang dapat dihitung dalam waktu wajar pada komputer standar (klasik), tetapi inversnya tidak dapat dihitung secara layak, disebut **fungsi satu arah** [atau **fungsi satu arah kriptografis**].

Perkalian dua bilangan, bahkan dua bilangan yang sangat besar, dapat dilakukan komputer dengan cukup cepat. Menentukan apakah bilangan yang sangat besar itu prima atau komposit juga ternyata sangat cepat (lihat [**AKS04**] untuk hasil mengagumkan dalam sejarah panjang uji keprimaan ini).

Namun, belum ditemukan cara klasik yang layak untuk *memfaktorkan* semiprima RSA yang cukup besar, yaitu hasil kali dua prima besar berukuran sebanding.[5] Pembatasan bentuk ini penting: bilangan genap atau bilangan dengan faktor kecil dapat difaktorkan dengan mudah, berapa pun besarnya. Sebagai contoh, salah satu semiprima RSA terbesar yang pernah difaktorkan pada saat naskah sumber ditulis adalah soal tantangan terkenal **RSA-768**, sebuah bilangan komposit 232 digit (768 bit). Bilangan itu akhirnya difaktorkan pada 2009 setelah jaringan berisi ratusan komputer bekerja bersama selama sekitar dua tahun, meskipun tidak secara eksklusif mengerjakan soal tersebut. Semiprima RSA sejenis yang lebih besar mudah dibuat, tetapi pada umumnya jauh lebih sulit difaktorkan.

Karena itu, fungsi yang mengalikan dua bilangan prima besar berukuran sebanding untuk menghasilkan semiprima yang sangat besar merupakan calon fungsi satu arah kriptografis yang baik.

Pada 1978, Ron Rivest, Adi Shamir, dan Leonard Adleman menjelaskan ([**RSA78**]) kriptosistem kunci publik berikut yang didasarkan pada fungsi satu arah tersebut.

DEFINISI 4.4.5. Bob memulai dengan memilih dua bilangan prima sangat besar yang berbeda, p dan q. Hasil kalinya $n = pq$ disebut **modulus RSA** yang bersesuaian. Bob juga memilih bilangan e yang memenuhi $1 < e < \phi(n)$ dan $\gcd(e, \phi(n)) = 1$. Bilangan e biasanya memiliki sangat sedikit angka 1 ketika ditulis dalam basis dua, misalnya 3 atau $65537 = 10000000000000001_2$. Bilangan ini disebut **eksponen RSA**.

Kunci publik [**enkripsi**] **RSA** k_e terdiri atas pasangan (n, e); himpunan semua pasangan semacam itu adalah $\mathcal{K}_e$.

Kunci privat [**dekripsi**] **RSA** k_d terdiri atas pasangan (n, d), dengan d dipilih sebagai wakil positif terkecil dari

$$d = e^{-1} \pmod{\phi(n)},$$

dan $\mathcal{K}_d$ adalah himpunan semua pasangan semacam itu.

Algoritme pembangkitan kunci RSA Gen memilih p, q, e seperti di atas, menghitung $n = pq$ dan $d = e^{-1} \pmod{\phi(n)}$, lalu menghasilkan pasangan $(k_e, k_d) = ((n, e), (n, d))$. Data faktor p, q (atau $\phi(n)$) digunakan pada tahap penyiapan dan tidak perlu menjadi bagian kunci dekripsi operasional.

Ruang pesan kriptosistem ini adalah $\mathcal{M} = \{m \in \mathbb{Z} \mid 0 \leq m < n\}$.

Enkripsi diberikan oleh

$$c = e_{(n,e)}(m) = m^e \pmod{n}\ .$$

Dekripsi diberikan oleh

$$d_{(n,d)}(c) = c^d \pmod{n}\ .$$

Keseluruhan sistem di atas disebut **kriptosistem RSA**.

[5]Pernyataan ini berlaku untuk komputer *klasik*. Terdapat algoritme pemfaktoran yang efisien pada *komputer kuantum* ; lihat [**Sho94**] dan [**NC10**].

Secara grafis:

Penyiapan dan notasi kriptosistem RSA:

Alice	pada jaringan publik	Bob
		pilih prima besar berbeda p dan q hitung **modulus RSA** $n = pq$ pilih **eksponen RSA** $e \in \mathbb{N}$ dengan $1 < e < \phi(n)$ dan $\gcd(e, \phi(n)) = 1$
unduh k_e	$\leftarrowtail$ kunci publik k_e $\leftarrowtail$	terbitkan $k_e = (n, e)$ hitung $d = e^{-1} \pmod{\phi(n)}$
pesan $m \in \mathcal{M}$ hitung $c = e_{(n,e)}(m)$ $= m^e \pmod{n}$ kirim c	$\rightarrowtail$ cipherteks c $\rightarrowtail$	terima c hitung $m = d_{(n,d)}(c)$ $= c^d \pmod{n}$

Pertama-tama, kita perlu memastikan bahwa sistem ini memenuhi syarat dasar agar berfungsi sebagai kriptosistem.

PROPOSISI 4.4.6. *Gunakan notasi dalam definisi kriptosistem RSA di atas. Untuk setiap pesan $m \in \mathcal{M}$, berlaku $d_{(n,d)}(e_{(n,e)}(m)) = m$.*

BUKTI. Setiap $m \in \mathcal{M}$ mewakili suatu kelas dalam $\mathbb{Z}/n\mathbb{Z}$. Kita tidak akan membedakan kelas tersebut dari wakilnya m yang memenuhi $0 \leq m < n$.

Kita membentuk d sebagai $d = e^{-1} \pmod{\phi(n)}$. Artinya, $e \cdot d \equiv 1 \pmod{\phi(n)}$, sehingga terdapat $k \in \mathbb{Z}$ dengan $e \cdot d = 1 + k\phi(n)$.

Kemudian, menurut Teorema Euler 3.3.4 , untuk setiap $m \in \mathcal{M}$ yang memenuhi $\gcd(m, n) = 1$, berlaku

$$d_{(n,d)}(e_{(n,e)}(m)) \equiv (m^e)^d = m^{ed} = m^{1+k\phi(n)} \equiv m \cdot (m^{\phi(n)})^k \equiv m \cdot (1)^k \equiv m \pmod{n}$$

seperti yang diinginkan. Kasus $\gcd(m, n) \neq 1$ menjadi Latihan 4.4.1 dalam bagian ini. □

Selain memastikan fungsi dasarnya, kita perlu menilai seberapa praktis RSA. Mari kita telusuri dengan cermat algoritme yang diperlukan pada setiap langkah.

(1) Bob harus memilih prima besar p dan q. Seperti telah disebutkan, terdapat algoritme yang dapat menentukan keprimaan suatu bilangan dalam waktu wajar. Lebih tepatnya, komputer (klasik) dapat menentukan apakah bilangan k prima

dalam waktu yang dibatasi oleh suatu fungsi polinomial dari $\log(k)$. [Inilah arti lazim *komputasi layak* dalam kriptologi.]

(2) Selain itu, jumlah prima cukup banyak sehingga Eve tidak dapat melakukan pencarian brute force atas semua kemungkinan. Hal ini mengikuti Teorema Bilangan Prima, yang memberikan banyaknya prima secara asimtotik.

TEOREMA 4.4.7. *Untuk $x \in \mathbb{R}$ dengan $x > 0$, definisikan* **fungsi penghitung prima** *sebagai $\pi(x) = \#\{p \in \mathbb{N} \mid p \text{ prima dan } p \leq x\}$. Maka*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Teorema ini merupakan salah satu permata teori bilangan analitik. Teorema ini dibuktikan pada 1896 oleh Jacques Hadamard dan Charles Jean de la Vallée-Poussin, walaupun bagian-bagian pentingnya telah diketahui sebelumnya oleh tokoh seperti Euler, Legendre, dan Riemann. Buktinya sulit, bahkan bukti *elementer* yang diberikan Atle Selberg dan Paul Erdös pada 1948.

Salah satu akibat Teorema Bilangan Prima ialah bahwa peluang sebuah bilangan k yang dipilih secara acak adalah prima kira-kira $1/\ln(k)$. Sebagai contoh, untuk mencari prima 200 digit, kita memilih bilangan acak berukuran itu dan perlu menguji sekitar $\ln(10^{200}) = 461$ bilangan sebelum memperoleh suatu prima. Jumlah komputasi ini masih wajar.

(3) Setelah memiliki modulus RSA $n = pq$, kita dapat menghitung fungsi totient Euler $\phi(n) = (p-1)(q-1)$ hampir seketika dengan Teorema 2.5.3.

(4) Menentukan eksponen RSA e yang relatif prima terhadap $\phi(n)$ tidak sulit karena terdapat banyak pilihan. Bahkan, dalam arti yang tepat, peluang bahwa dua bilangan yang dipilih secara acak saling relatif prima adalah $\frac{6}{\pi^2}$ (untuk pernyataan tepat beserta buktinya, lihat [**HW79**]). Pengujian calon e juga efisien sebab, seperti akan kita lihat dalam Latihan 4.4.3, waktu Algoritma Euklides dibatasi oleh fungsi polinomial dari logaritma bilangan-bilangan yang terlibat. Jadi, komputasinya *layak*.

(5) Selanjutnya, $d = e^{-1} \pmod{\phi(n)}$ dapat dihitung sangat cepat dengan Algoritma Euklides diperluas (Teorema 1.6.2). Algoritme ini tentu lebih lambat daripada Algoritma Euklides dasar, tetapi tetap layak.

(6) Enkripsi dan dekripsi RSA sama-sama berupa pemangkatan suatu bilangan modulo n. Untungnya, terdapat algoritme bernama **eksponensiasi modular cepat** yang juga menyelesaikannya dalam waktu yang dibatasi oleh fungsi polinomial dari logaritma bilangan-bilangan yang diberikan.

(7) Persoalan praktis terakhir ialah cara Alice benar-benar menggunakan RSA untuk mengirim pesan yang diinginkannya, bukan sekadar bilangan $m \in \mathbb{Z}$ yang memenuhi $0 \leq m < n$.

Ini merupakan persoalan baku dalam kriptografi matematis dan mempunyai solusi baku. Biasanya, Alice harus mengambil pesannya karakter demi karakter lalu menyalinnya menjadi barisan bilangan menurut suatu standar yang diterima. Sejak dekade 1960-an, hal ini dilakukan menggunakan **kode ASCII** [American Standard Code for Information Interchange, Kode Standar Amerika untuk Pertukaran Informasi] . ASCII memberikan bilangan biner 7 bit untuk 26 huruf alfabet Latin (modern), baik huruf besar maupun kecil, serta untuk sekumpulan simbol yang lazim dan beberapa tambahan modern yang biasanya tidak dicetak, seperti 11110_2 *Pemisah Rekaman*, 111_2 *Bel*, dan 1011_2 *Tab Vertikal*. Kini, kode-kode ASCII selalu disimpan dalam satu byte (8 bit) dengan menambahkan bit 0 di depan.

Ketika World Wide Web menjadi fenomena global, kebutuhan akan lebih banyak alfabet dan bahkan sistem tulisan nonalfabetis (seperti aksara Tionghoa) terus meningkat. Hal ini menghasilkan sistem bernama **Unicode** yang, pada versi 6.3 tahun 2013, memuat lebih dari 110.000 karakter. Unicode disimpan dengan berbagai pengodean. Dua yang paling umum adalah **UTF-8**, yang menggunakan satu hingga empat byte per karakter, dan **UTF-16**, yang menggunakan dua atau empat byte per karakter.

Jadi, Alice biasanya menuliskan pesannya dalam ASCII atau Unicode, menyambungkan semua byte secara berurutan, lalu memotong seluruh pesan menjadi blok-blok sepanjang b bit. Di sini $b \in \mathbb{N}$ dipilih sebagai nilai terbesar yang memenuhi $2^b < n$. Dengan demikian, setiap blok b bit dapat dipandang sebagai bilangan bulat $m \in \mathbb{Z}$ yang memenuhi $0 \leq m < n$, sehingga RSA dapat diterapkan pada pesan tersebut satu blok demi satu blok.

(Kita mengabaikan banyak perincian, misalnya cara menyisakan ruang untuk salt, pendekatan lain, dan persoalan struktur blok. Lihat referensi baku tentang kriptografi, seperti [**FS03**] atau [**MVOV96**].)

Latihan untuk §4.4.

LATIHAN 4.4.1. Dalam soal ini, Anda akan menyelesaikan bukti Proposisi 4.4.6, yang menyatakan bahwa dekripsi RSA berfungsi dengan benar dalam semua kasus.

Sebagai langkah pertama, nyatakan secara formal dan buktikan sebuah lema: untuk prima berbeda p dan q, dua bilangan bulat r dan s kongruen modulo pq jika dan hanya jika keduanya kongruen modulo p dan modulo q. *[Petunjuk: Teorema Sisa Cina.]*

Sekarang, gunakan hasil di atas untuk membuktikan kasus yang belum dibuktikan dalam Proposisi 4.4.6. Diberikan prima berbeda p dan q, tetapkan $n = pq$. Misalkan $e \in \mathbb{N}$ memenuhi $\gcd(e, \phi(n)) = 1$ dan $d \in \mathbb{N}$ merupakan invers e modulo $\phi(n)$. Buktikan bahwa untuk setiap $m \in \mathbb{Z}$ yang memenuhi $0 \leq m < n$ dan $\gcd(m, n) \neq 1$, berlaku $m^{ed} \equiv m \pmod{n}$.

LATIHAN 4.4.2. Berapa banyak komputasi yang diperlukan untuk menghitung $a^k \pmod{n}$ bagi $a \in \mathbb{Z}$ dan $k, n \in \mathbb{N}$ dengan $n \geq 2$?

Misalkan D adalah panjang maksimum masukan a, k, dan n, diukur dalam digit. Perkalian dua bilangan merupakan instruksi dasar pada sebagian besar komputer modern dan dapat dianggap memerlukan satu satuan waktu. (Atau, Anda dapat melakukan sejumlah manipulasi lebih kecil yang banyaknya dibatasi oleh fungsi polinomial dari panjang operan; pilihan ini tidak memengaruhi bagian selanjutnya dari soal.) Demikian pula, pembagian bersisa merupakan satu instruksi mesin (misalnya pada prosesor keluarga Pentium) atau dapat dilakukan dengan cara sekolah dasar dalam waktu polinomial terhadap panjang masukannya.

Anggaplah pekerjaan untuk melakukan satu perkalian lalu mereduksi modulo n dibatasi oleh fungsi polinomial $p(D)$.

Jika kita sekadar membentuk k faktor a, melakukan $k - 1$ perkalian, dan mereduksi modulo n pada setiap langkah, waktunya berorde $O(kp(D))$. Karena bilangan k yang terdiri atas D digit dapat berorde 10^D, batas waktu ini bersifat *eksponensial* terhadap panjang masukan D.

Cobalah menemukan algoritme eksponensiasi yang jauh lebih cepat, dengan waktu polinomial alih-alih eksponensial.

[Petunjuk: (1) Buat tabel kuadrat berulang dari a modulo n, yaitu a^2, a^4, a^8, dan seterusnya. (2) Tuliskan k dalam basis dua dan uraikan a^k menggunakan bentuk biner k, aturan pemangkatan biasa, dan tabel tersebut. Hasil akhirnya harus mendeskripsikan cara menghitung $a^k \pmod{n}$; periksa dengan cermat berapa banyak waktu yang diperlukan.]

LATIHAN 4.4.3. Untuk $k \in \mathbb{N}$, lakukan permainan berikut:

(1) gunakan Algoritma Pembagian untuk membagi k dengan dua dan memperoleh hasil bagi q serta sisa r;
(2) ganti $k \leftarrow q$;

(3) jika $k > 0$, ulangi dari langkah (1); jika tidak, berhenti.

Berikan batas banyaknya langkah sampai permainan ini berhenti. Nyatakan jawaban sebagai fungsi dari k, fungsi dari banyaknya bit yang diperlukan untuk menuliskan k dalam basis dua, atau fungsi dari banyaknya digit yang diperlukan untuk menuliskan k dalam basis 10.

Tunjukkan bahwa setiap dua langkah Algoritma Euklides membuat suku-suku sisa r_i berkurang sekurang-kurangnya dengan faktor $1/2$. Dengan kata lain, jika kita menggunakan notasi Teorema 1.6.2, maka $r_{j+2} < \frac{1}{2} r_j$ untuk setiap $j \in \mathbb{Z}$ yang memenuhi $j \geq 0$.

Jelaskan mengapa hal ini berarti Algoritma Euklides memerlukan paling banyak $2\lfloor \log_2(b) \rfloor + 1$ langkah pembagian untuk menghitung $\gcd(a, b)$. Turunkan pula batas linear sebesar paling banyak tujuh kali banyaknya digit desimal b, dengan memeriksa kasus ujung kecil secara terpisah. *[Petunjuk: berapakah* $\log_2(10)$*?]*

Jelaskan mengapa hasil ini berarti Algoritma Euklides merupakan komputasi yang *layak* secara kriptologis, dalam pengertian bagian ini.

4.5. Tanda Tangan Digital

Kriptosistem kunci publik memungkinkan beberapa penggunaan yang tidak tersedia pada kriptosistem simetris. Salah satu penggunaan yang makin penting dalam ekonomi digital modern ialah pembuatan *tanda tangan digital*: bagian dari dokumen elektronik yang diharapkan memiliki salah satu sifat tanda tangan fisik, yakni sulit dipalsukan oleh penyamar. Dokumen bertanda tangan semacam itu mungkin diperlukan, misalnya, jika Bob dari bagian sebelumnya (yang memasang kunci publik RSA-nya di situs web) hendak mengirim kontrak yang mengikat secara hukum melalui surel. Barangkali Alice dan Bob ingin mengirim kepada calon pemilik rumah mereka, Larry, perjanjian sewa bertanda tangan untuk apartemen yang akan mereka tinggali bersama. Ketika menerima surel dari Bob yang berbunyi "Saya setuju terikat oleh ketentuan perjanjian sewa ini," Larry perlu yakin bahwa surel tersebut benar-benar berasal dari Bob; tanda tangan digital dapat memberikan keyakinan itu.

Untuk skema dasar berikut, kita memerlukan sifat tambahan. Setiap pesan yang hendak ditandatangani harus berada dalam domain operasi privat d_{k_d}; untuk setiap pasangan (k_e, k_d) yang dihasilkan Gen dan setiap $m \in \mathcal{M}$, harus berlaku $e_{k_e}(d_{k_d}(m)) = m$, seperti pada RSA. Definisi umum kriptosistem asimetris sebelumnya hanya mensyaratkan urutan sebaliknya.

Bob lalu dapat melakukan hal berikut. Ia mengambil salinan perjanjian sewa, menambahkan bagian di akhir yang menyatakan persetujuannya atas ketentuan tersebut dan memuat informasi pengenal pribadi (mungkin pindaian surat izin mengemudinya). Sebut seluruh bongkah data ini m. Bob kemudian menerapkan algoritme *dekripsi* dengan kunci privat (dekripsi) k_d, sehingga diperoleh $s = d_{k_d}(m)$. Nilai s ini disebut tanda tangan Bob atas pesan m. Ia lalu mengirimkan m dan s kepada Larry melalui surel.

Ketika menerima pesan bertanda tangan ini, Larry mula-mula memisahkan tanda tangan s, lalu menghitung enkripsinya, $e_{k_e}(s)$, menggunakan kunci publik yang ia unduh dari situs web Bob. Berdasarkan sifat tambahan di atas, hasilnya harus sama dengan m. Verifikasi $e_{k_e}(s) = m$ itu sendiri hanya menetapkan konsistensi aljabar pasangan (m, s) terhadap kunci publik tersebut. Untuk menyimpulkan bahwa Bob menghasilkan tanda tangan dan bahwa pesan tidak berubah sejak ditandatangani, Larry juga harus mengandalkan skema tanda tangan yang tak dapat dipalsukan, kunci privat Bob yang tidak terkompromi, serta pengikatan tepercaya antara identitas Bob dan kunci publik tersebut. Bahkan dengan asumsi-asumsi itu, verifikasi tidak dengan sendirinya membuktikan identitas pengirim surel ataupun kebaruan pesan, sebab pasangan bertanda tangan yang lama dapat diteruskan atau diputar ulang oleh siapa pun.

Secara grafis:

Tanda tangan digital dasar:

Larry	pada jaringan publik	Bob
		jalankan Gen untuk memperoleh $(k_e, k_d) \in \mathcal{K}_e \times \mathcal{K}_d$
unduh k_e	$\longleftarrow$ kunci publik k_e $\longleftarrow$	terbitkan k_e
		pesan $m \in \mathcal{M}$
		hitung $s = d_{k_d}(m)$
terima (m, s)	$\longleftarrow$ pesan bertanda tangan (m, s) $\longleftarrow$	kirim (m, s)
jika $e_{k_e}(s) = m$ TERIMA jika tidak, TOLAK		

Salah satu masalah skema ini ialah ukuran pesan secara efektif menjadi dua kali lipat. Tanda tangan yang lebih kecil dan efisien dapat dibuat dengan mendekripsi bukan seluruh m, melainkan nilai suatu fungsi $h(m)$. Fungsi h harus menerima pesan berukuran sebarang dan menghasilkan ringkasan data yang kecil, tetapi tetap bergantung pada setiap bagian masukan m. Bagaimanapun, jika $h(m)$ hanya bergantung pada 100 bit pertama m, misalnya, Eve yang berniat jahat dapat mengubah pesan selama pengiriman tanpa terdeteksi selama ia tidak mengubah 100 bit pertama pesan tersebut.

Kriptolog mempunyai nama untuk fungsi seperti h ini.

DEFINISI 4.5.1. Fungsi h yang menerima string bit berpanjang sebarang dan menghasilkan string bit berpanjang tetap disebut **fungsi hash kriptografis** jika memenuhi

kemudahan komputasi: nilai $h(m)$ dapat dihitung secara layak untuk setiap m;

ketahanan praimaji: jika masukan tantangan M dipilih secara acak menurut distribusi yang ditetapkan dan hanya nilai target $t = h(M)$ yang diberikan, mencari m sedemikian sehingga $h(m) = t$ tidak layak dilakukan;

ketahanan praimaji kedua: jika diberikan masukan tertentu m_1, mencari masukan lain m_2 sedemikian sehingga $h(m_2) = h(m_1)$ tidak layak dilakukan;

ketahanan tumbukan: mencari dua pesan berbeda $m_1 \neq m_2$ sedemikian sehingga $h(m_2) = h(m_1)$ tidak layak dilakukan .

Kata *layak* dan *tidak layak* di sini bermakna sama seperti pada bagian sebelumnya: komputasi tersebut dapat atau tidak dapat diselesaikan dalam waktu yang dibatasi oleh suatu fungsi polinomial dari ukuran masukan.

Perhatikan bahwa karena fungsi hash menerima masukan berpanjang sebarang tetapi mempunyai ukuran keluaran tetap, pasti terdapat tak hingga banyak tumbukan.

Pembuatan fungsi hash kriptografis sedikit menyerupai seni gelap. Ternyata, jika suatu calon fungsi hash dibangun dengan struktur yang jelas (biasanya struktur matematis), terutama bila fungsi itu cepat dihitung, komunitas kriptologi biasanya menemukan cara

untuk menembus salah satu syarat ketahanannya. Karena itu, algoritme yang digunakan secara luas cenderung berupa komputasi yang sangat *ad hoc*, tampak rumit, dan sejauh ini bertahan terhadap upaya membalikkan fungsi atau mematahkan sifat ketahanannya.

CONTOH 4.5.2. Selama kira-kira satu dasawarsa sejak awal 1990-an, fungsi hash kriptografis yang paling luas digunakan bernama `md5`. Algoritme ini dikembangkan oleh Ron Rivest dan diterbitkan pada 1992. Ukuran keluaran `md5` adalah 128 bit.

Walaupun `md5` telah dicurigai memiliki kelemahan sejak pertengahan 1990-an, serangan nyata baru diterbitkan pada 2004, ketika ditunjukkan bahwa fungsi ini tidak tahan tumbukan[**WY05**]. Pada saat naskah sumber ini ditulis, `md5` masih digunakan secara luas untuk memeriksa apakah transfer data berukuran besar mengalami galat transmisi; dengan kata lain, fungsi ini tetap berguna untuk menguji kerusakan data yang tidak disengaja. (Dalam konteks pembuktian integritas data terhadap kerusakan yang tidak disengaja ini, fungsi hash sering disebut **sidik jari**.)

CONTOH 4.5.3. Sejak akhir 1990-an hingga tidak lama sebelum naskah sumber ini ditulis, fungsi hash kriptografis yang paling luas digunakan dan ditanamkan dalam banyak protokol kriptografis yang diterima luas serta distandardisasi adalah `SHA-1`, dengan ukuran keluaran 160 bit.

`SHA-1` dikembangkan oleh Badan Keamanan Nasional Amerika Serikat (NSA) melalui proses yang sebagian terbuka, lalu diadopsi oleh Institut Standar dan Teknologi Nasional Amerika Serikat (NIST) sebagai bagian dari beberapa Standar Pemrosesan Informasi Federal Amerika Serikat .

Pada 2004, diterbitkan sejumlah penelitian yang menunjukkan bahwa `SHA-1` mungkin rentan terhadap jenis serangan tertentu. (Lihat [**PS04**].) Karena itu, pada 2010 NIST mewajibkan banyak aplikasi perlindungan data federal Amerika Serikat beralih ke fungsi hash lain.

CONTOH 4.5.4. Pada saat naskah sumber ini ditulis, sebagian besar pengguna dan organisasi yang memerhatikan keamanan merekomendasikan `SHA-2`, biasanya dalam varian "`SHA-256`" yang memiliki ukuran keluaran 256 bit. Mengingat pengungkapan ketika itu mengenai keterlibatan NSA dalam protokol kriptografis dan pelemahan protokol tersebut, partisipasi NSA dalam pengembangan `SHA-2` mungkin menimbulkan kekhawatiran.

Untuk menerapkan operasi RSA pada keluaran bit $h(m)$, terlebih dahulu gunakan enkode tanda tangan yang disepakati untuk memperoleh wakil pesan $H_n(m) \in \mathcal{M} = \{0, \ldots, n-1\}$. Skema RSA standar menggunakan enkode dan padding khusus sebelum menerapkan operasi privat; diagram berikut hanya menunjukkan alur matematis skematis dan bukan konstruksi yang siap dipakai.

Secara grafis:

Tanda tangan digital RSA:

Charlie	pada jaringan publik	Bob
		lakukan penyiapan RSA, buat $k_e = (n, e)$ dan d
unduh k_e	$\leftarrowtail$ kunci verifikasi k_e $\leftarrowtail$	terbitkan k_e
		pesan $m \in \mathcal{M}$
		hitung $s = (H_n(m))^d \pmod n$
terima (m, s)	$\leftarrowtail$ pesan bertanda tangan (m, s) $\leftarrowtail$	kirim (m, s)
jika $H_n(m) = s^e \pmod n$		
TERIMA		
jika tidak, TOLAK		

Dengan pemahaman ini, kita dapat mendeskripsikan tanda tangan digital secara lebih formal.

DEFINISI 4.5.5. Misalkan Bob menyiapkan kriptosistem RSA seperti dalam Definisi 4.4.5, lalu memilih satu fungsi hash kriptografis h dan enkode wakil pesan H_n untuk digunakan seterusnya. Ia menerbitkan deskripsi keduanya di halaman web bersama kunci enkripsi publik k_e.

Jika Bob hendak menandatangani pesan m, sebelum mengirimkannya kepada pihak ketiga, misalnya Charlie, ia menambahkan **tanda tangan digital RSA** $s = d_{k_d}(H_n(m)) = (H_n(m))^d \pmod n$ pada m.

Ketika menerima pesan bertanda tangan (m, s) yang mengaku berasal dari Bob, Charlie membuka situs web Bob dan mengunduh kunci publik k_e beserta deskripsi h dan H_n. Charlie kemudian menghitung $e_{k_e}(s) = s^e \pmod n$ dan membandingkannya dengan $H_n(m)$. Jika keduanya sama, ia **menerima** tanda tangan tersebut; jika tidak, ia **menolaknya**.

Dalam konteks ini, kunci privat/dekripsi Bob k_d disebut **kunci penandatanganan**, sedangkan kunci publik/enkripsi k_e disebut **kunci verifikasi**.

Latihan untuk §4.5.

LATIHAN 4.5.1. Gunakan Prinsip Sarang Merpati (Teorema 1.1.2) untuk membuktikan bahwa fungsi hash kriptografis selalu mempunyai tak hingga banyak tumbukan [meskipun tumbukan tersebut belum tentu dapat ditemukan secara layak].

LATIHAN 4.5.2. Berikan contoh fungsi hash h dengan keluaran berukuran satu bit dan masukan tertentu m_1 yang tidak mempunyai praimaji kedua; yakni, tidak ada $m_2 \neq m_1$ sedemikian sehingga $h(m_2) = h(m_1)$.

4.6. Serangan Man-in-the-Middle, Sertifikat, dan Kepercayaan

Kripto kunci publik dapat tampak sebagai manfaat tanpa cela bagi dunia berjejaring. Namun, pemeriksaan cermat atas dua bagian sebelumnya menunjukkan kesenjangan berbahaya antara gambaran sederhana mengenai sifat alat kriptografis itu dan kenyataannya. Perbedaan yang mula-mula luput dari perhatian ialah antara *Bob sebagai orang* dan *bit-bit* yang tiba melalui jaringan ke Alice atau Larry sambil *mengaku berasal dari Bob*. Perbedaan ini tidak banyak berpengaruh jika Eve hanya menjadi pengamat pasif komunikasi antara Alice dan Bob (dan kadang-kadang Larry), seperti yang selama ini umumnya kita asumsikan. Namun, jika Eve menguasai jaringan lebih jauh dan dapat mengganti semua komunikasi dengan versinya sendiri, serangan baru menjadi mungkin.

Misalkan Alice ingin mengirim pesan rahasia kepada Bob tanpa pernah bertemu dengannya untuk bertukar kunci kriptosistem simetris. Ia berharap Bob mempunyai kunci publik, lalu mengakses web dan mengunduh halaman utama Bob.

Pada titik inilah Eve bertindak. Ia mencegat respons Bob (tepatnya, server web Bob) terhadap permintaan tersebut. Eve menyimpan salinan kunci publik Bob k_e^B, tetapi mengganti kunci itu dalam data halaman web dengan kunci enkripsi RSA milik Eve, k_e^E; hanya Eve yang mengetahui kunci dekripsi pasangannya, k_d^E. Ia kemudian meneruskan halaman yang telah diubah kepada Alice.

Alice menyusun teks terang m dan mengirim cipherteks yang bersesuaian, $c_A = e_{k_e^E}(m)$, kepada Bob—setidaknya demikian menurutnya. Eve justru mencegat cipherteks itu, mendekripsinya, lalu menyimpan $m = d_{k_d^E}(c_A) = d_{k_d^E}(e_{k_e^E}(m))$. Agar Alice dan Bob mengira semuanya berjalan normal (dan terus bercakap-cakap sambil membocorkan informasi), Eve meneruskan $c_E = e_{k_e^B}(m)$ kepada Bob.

Dari sudut pandang Bob, ia menerima surel yang tampak berasal dari Alice dan yang, setelah didekripsi dengan kunci privatnya, sepenuhnya masuk akal. Bahkan, jika ia berinteraksi dengan Alice di luar jaringan, Alice bertindak seolah-olah memang mengirim pesan itu. Alice memang mengirimnya, tetapi bukan dalam bentuk terenkripsi yang diterima Bob. Eve telah sepenuhnya melanggar *kerahasiaan* komunikasi Alice dan Bob. Ia juga dapat merusak *integritas* pesan kapan pun ia mau sambil tetap membuatnya tampak sah berasal dari Alice.

Skenario di atas disebut **serangan man-in-the-middle** (istilah konvensional ini memang tidak netral gender).

Berikut gambaran grafis serangan tersebut:

Serangan man-in-the-middle:

Alice	Eve	Bob
	cegat $k_e^B \leftarrowtail$	bangkitkan kunci: publik k_e^B, privat k_d^B terbitkan k_e^B
unduh k_e^E	bangkitkan kunci: publik k_e^E, privat k_d^E $\leftarrowtail k_e^E$, palsukan sumber	
pesan $m \in \mathcal{M}$ hitung $c_A = e_{k_e^E}(m)$ kirim c_A	$\rightarrowtail c_A$, cegat	
	ambil teks terang $m = d_{k_d^E}(c_A)$ ubah menjadi m' jika diinginkan hitung $c_E = e_{k_e^B}(m')$ palsukan sumber $c_E \rightarrowtail$	terima c_E
		baca pesan $m' = d_{k_d^B}(c_E)$

Jadi, kriptosistem simetris ternyata mempunyai satu keuntungan bawaan. Ketika para pihak bertemu pada saat ideal untuk bertukar kunci simetris, mereka semestinya dapat memastikan identitas lawan bicara. Jika tidak, mereka tentu tidak akan bertukar kunci sebelum memeriksa cukup banyak dokumen identitas yang terlihat resmi. Kriptosistem asimetris harus mengatasi kesulitan mendasar: membangun hubungan tepercaya antara identitas orang nyata dan kunci publik di Internet yang mengaku berasal dari orang tersebut.

Teknik dari bagian sebelumnya, §4.5, setidaknya dapat membantu memindahkan kepercayaan. Misalkan Alice ingin berkomunikasi secara rahasia dengan Bob, tetapi tidak tahu apakah kunci publik yang tampak berada di halaman web Bob dapat dipercaya. Jika kunci tersebut disertai tanda tangan digital yang diterbitkan oleh *pihak ketiga tepercaya* [TTP] dan Alice telah memperoleh kunci publik TTP sebagai jangkar kepercayaan melalui kanal yang diautentikasi secara independen—atau dapat memvalidasi jalur sertifikasi hingga jangkar semacam itu—ia dapat memverifikasi pengikatan kunci tersebut dengan identitas Bob, setidaknya sejauh yang telah diperiksa dan dinyatakan oleh TTP.

Berikut definisi formalnya.

DEFINISI 4.6.1. Individu atau organisasi yang ingin menggunakan kriptografi asimetris dapat meminta pihak ketiga tepercaya yang disebut **otoritas sertifikat** [**CA**] menerbitkan **sertifikat digital** bagi kunci publiknya. Sertifikat merupakan pernyataan terstruktur yang mengikat identitas subjek dengan kunci publiknya (beserta metadata yang diperlukan), lalu

ditandatangani menggunakan kunci penandatanganan CA. Kunci verifikasi CA diasumsikan tersebar luas di Internet atau dipasang dalam perangkat lunak sistem operasi maupun perangkat keras komputer. Penyebaran luas saja tidak membuat kunci tersebut tepercaya. Kunci verifikasi CA hanya dapat menjadi dasar kepercayaan jika diperoleh sebagai jangkar kepercayaan yang diautentikasi secara independen, atau jika dapat divalidasi melalui jalur sertifikasi yang berujung pada jangkar semacam itu. Siapa pun yang hendak memakai suatu kunci publik dapat terlebih dahulu memeriksa keabsahan sertifikat terkait dan menilai pengikatan identitas–kunci itu berdasarkan kebijakan serta pemeriksaan CA.

Keseluruhan ekosistem sertifikat, CA, jangkar kepercayaan, mekanisme distribusi dan validasi, dan seterusnya, disebut **infrastruktur kunci publik** atau **PKI**.

Dalam praktik yang dibahas naskah sumber, CA sering kali hanya dapat menyertifikasi bahwa suatu kunci publik dikuasai oleh orang yang mempunyai akses ke alamat surel tertentu, kata sandi pengelola situs tertentu, atau token lain yang sepenuhnya berbasis Internet. Pemeriksaan itu biasanya mudah. Mengaitkannya dengan identitas nyata di luar jaringan mungkin memerlukan pemeriksaan dokumen identitas resmi dan jarang dilakukan. Naskah sumber juga mengusulkan kemungkinan peran pemerintah sebagai CA serta dokumen identitas ber-RFID yang dapat mengirimkan sertifikat bagi kunci publik pemiliknya (paspor Amerika Serikat yang lebih baru ketika itu telah memakai RFID).

Ada pendekatan lain untuk menentukan apakah suatu kunci publik dapat dipercaya, yang disukai orang-orang yang tidak memercayai otoritas terpusat tetapi bersedia memercayai orang tertentu yang mereka kenal langsung. Dalam pendekatan ini, orang-orang yang saling mengenal dan telah memverifikasi identitas serta kunci satu sama lain dapat menandatangani pengikatan identitas–kunci tersebut, menambahkan tanda tangan digital pada kumpulan yang sudah ada. Ketika hendak memakai kunci publik seseorang, Anda dapat menelusuri rantai tanda tangan digital, masing-masing mengesahkan pengikatan berikutnya, hingga mencapai orang yang Anda kenal langsung dan yang kuncinya telah Anda verifikasi.

Tanda tangan yang valid hanya menunjukkan bahwa suatu kunci menyertifikasi pengikatan identitas–kunci berikutnya; validitas itu sendiri belum membuat penyertifikasi tersebut layak dipercaya sebagai pengenal. Pengguna tetap harus menetapkan kebijakan kepercayaan lokal, termasuk seberapa jauh ia memercayai ketelitian setiap penyertifikasi dalam mengesahkan orang lain (*ownertrust*), lalu menerima suatu pengikatan hanya jika sertifikasi yang ada memenuhi kebijakan tersebut.

Pendekatan ini dikenal sebagai **jejaring kepercayaan** (*web of trust*) . Pendekatan tersebut didukung kuat oleh `GnuPG` dan perangkat lain yang kompatibel dengan `OpenPGP`; lihat `gnupg.org`.

Agar berguna, jejaring kepercayaan memerlukan sertifikasi yang telah diverifikasi dan memenuhi kebijakan kepercayaan lokal serta penilaian *ownertrust*; sekadar menambah

sebanyak mungkin tanda tangan tanpa verifikasi tidak memperkuat kepercayaan. Salah satu cara membangun sertifikasi tersebut ialah mengadakan **pertemuan penandatanganan kunci**. Pada pertemuan semacam itu, setiap penanda tangan harus memeriksa identitas pemilik kunci dan membandingkan sidik jari kunci lengkap secara langsung. Pernyataan pihak lain saja tidak cukup. Gunakan algoritme sidik jari yang diwajibkan format kunci yang berlaku, bukan `md5`, karena `md5` tidak lagi aman terhadap tumbukan.

BAB 5

Indeks = Logaritma Diskret

Kita telah membahas *subgrup siklik* $\langle a \rangle$ *dari* $(\mathbb{Z}/n\mathbb{Z})^*$ *yang dibangkitkan oleh unsur* a dalam bukti versi Teorema Lagrange 3.3.3, sebagai langkah menuju Teorema Euler 3.3.4. Ingat bahwa subgrup itu terdiri atas semua pangkat a (lebih tepatnya, $[a]_n$) dalam $(\mathbb{Z}/n\mathbb{Z})^*$. Berikut beberapa contoh:

n	$\phi(n)$	$(\mathbb{Z}/n\mathbb{Z})^*$	a	$\langle a \rangle$	$\mathrm{ord}_n(a)$
2	1	$\{1\}$	1	$\{1\}$	1
3	2	$\{1,\ 2\}$	1	$\{1\}$	1
			2	$\{2,\ 2^2 \equiv 1\}$	2
4	2	$\{1,\ 3\}$	1	$\{1\}$	1
			3	$\{3,\ 3^2 \equiv 1\}$	2
5	4	$\{1,\ 2,\ 3,\ 4\}$	1	$\{1\}$	1
			2	$\{2,\ 2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^4 \equiv 1\}$	4
			3	$\{3,\ 3^2 \equiv 4,\ 3^3 \equiv 2,\ 3^4 \equiv 1\}$	4
			4	$\{4,\ 4^2 \equiv 1\}$	2
6	2	$\{1,\ 5\}$	1	$\{1\}$	1
			5	$\{5,\ 5^2 \equiv 1\}$	2
7	6	$\{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$	1	$\{1\}$	1
			2	$\{2,\ 2^2 \equiv 4,\ 2^3 \equiv 1\}$	3
			3	$\{3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1\}$	6
			4	$\{4,\ 4^2 \equiv 2,\ 4^3 \equiv 1\}$	3
			5	$\{5,\ 5^2 \equiv 4,\ 5^3 \equiv 6,\ 5^4 \equiv 2,\ 5^5 \equiv 3,\ 5^6 \equiv 1\}$	6
			6	$\{6,\ 6^2 \equiv 1\}$	2
8	4	$\{1,\ 3,\ 5,\ 7\}$	1	$\{1\}$	1
			3	$\{3,\ 3^2 \equiv 1\}$	2
			5	$\{5,\ 5^2 \equiv 1\}$	2
			7	$\{7,\ 7^2 \equiv 1\}$	2

TABEL 5.0.1. Subgrup siklik dari $(\mathbb{Z}/n\mathbb{Z})^*$ untuk $n = 2, \ldots, 8$

Setiap subgrup siklik $\langle a \rangle$ ini mempunyai ukuran, yakni orde $\mathrm{ord}_n(a)$ dari pembangkitnya, yang membagi ukuran grup induk $(\mathbb{Z}/n\mathbb{Z})^*$, sebagaimana dijamin oleh versi Teorema Lagrange 3.3.3.

Dengan bukti yang masih sangat terbatas pada tabel ini, kita juga dapat membuat beberapa pengamatan sementara yang mungkin benar secara umum, mungkin juga tidak:

- sering kali terdapat unsur a yang membangkitkan subgrup siklik sebesar mungkin: $\langle a \rangle = (\mathbb{Z}/n\mathbb{Z})^*$;
- grup satuan $(\mathbb{Z}/n\mathbb{Z})^*$ tampaknya selalu mempunyai subgrup siklik sebesar itu ketika n prima;
- bahkan beberapa n komposit menghasilkan $(\mathbb{Z}/n\mathbb{Z})^*$ yang mempunyai subgrup siklik besar, kecuali pangkat 2 terbesar yang telah kita coba, yaitu $n = 2^3$.

Untuk melihat apakah dugaan umum sementara itu masih bertahan, mari kita hitung dua contoh lagi. Demi menghemat tempat, kita hanya mencantumkan ukuran $(\mathbb{Z}/n\mathbb{Z})^*$ dan $\langle a \rangle$, bukan daftar lengkap unsurnya; unsur-unsur $(\mathbb{Z}/n\mathbb{Z})^*$ sendiri dapat dibaca pada kolom berlabel "a":

n	$\phi(n)$	$a \in (\mathbb{Z}/n\mathbb{Z})^*$	$\mathrm{ord}_n(a)$
16	8	1	1
		3	4
		5	4
		7	2
		9	2
		11	4
		13	4
		15	2
17	16	1	1
		2	8
		3	16
		4	4
		5	16
		6	16
		7	16
		8	8
		9	8
		10	16
		11	16
		12	16
		13	4
		14	16
		15	8
		16	2

TABEL 5.0.2. Subgrup siklik dari $(\mathbb{Z}/n\mathbb{Z})^*$ untuk $n = 16$ dan $n = 17$

Dugaan kita (pangkat besar dari 2 kurang baik; nilai n lain, terutama yang prima, lebih baik) masih bertahan. Tentu saja, bukti empiris berhingga sebanyak apa pun belum dapat memastikan pernyataan matematika yang bersifat umum.

Sekarang kita beralih ke analisis formal.

5.1. Sifat-Sifat Lain Orde Multiplikatif

Sebelum itu, kita memerlukan beberapa fakta tambahan tentang orde [multiplikatif].

TEOREMA 5.1.1. *Misalkan $n \in \mathbb{N}$ dan $a \in \mathbb{Z}$ memenuhi $n \geq 2$ dan $\gcd(a, n) = 1$. Maka, untuk $k \in \mathbb{N}$, berlaku $a^k \equiv 1 \pmod{n}$ jika dan hanya jika $\mathrm{ord}_n(a) \mid k$.*

BUKTI. Satu arah sangat mudah: jika $k \in \mathbb{N}$ memenuhi $\mathrm{ord}_n(a) \mid k$, maka $\exists d \in \mathbb{N}$ sedemikian sehingga $k = \mathrm{ord}_n(a) \cdot d$. Jadi,

$$a^k = a^{\mathrm{ord}_n(a)\cdot d} = (a^{\mathrm{ord}_n(a)})^d \equiv 1^d = 1 \pmod{n}\,.$$

Sebaliknya, misalkan $k \in \mathbb{N}$ memenuhi $a^k \equiv 1 \pmod{n}$. Terapkan Algoritma Pembagian untuk memperoleh $q, r \in \mathbb{Z}_{\geq 0}$ sedemikian sehingga $k = \mathrm{ord}_n(a) \cdot q + r$ dan $0 \leq r < \mathrm{ord}_n(a)$. Maka

$$1 \equiv a^k = a^{\mathrm{ord}_n(a)\cdot q + r} = (a^{\mathrm{ord}_n(a)})^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{n}\,.$$

Namun, menurut definisi orde, $\mathrm{ord}_n(a)$ adalah bilangan bulat positif terkecil yang membuat a berpangkat bilangan tersebut kongruen dengan 1. Karena itu, $a^r \equiv 1 \pmod{n}$ dan $0 \leq r < \mathrm{ord}_n(a)$ hanya mungkin jika $r = 0$. Jadi, $k = \mathrm{ord}_n(a) \cdot q$ dan $\mathrm{ord}_n(a) \mid k$, seperti yang diinginkan. □

Artinya, ketika bekerja dalam subgrup siklik dari $(\mathbb{Z}/n\mathbb{Z})^*$ yang dibangkitkan oleh suatu unsur a, kita harus memperlakukan pangkat-pangkat a seolah-olah pangkat tersebut hidup dalam $\mathbb{Z}/(\mathrm{ord}_n(a))\mathbb{Z}$. Tepatnya:

TEOREMA 5.1.2. *Misalkan $n \in \mathbb{N}$ dan $a \in \mathbb{Z}$ memenuhi $n \geq 2$ dan $\gcd(a, n) = 1$. Maka, untuk $j, k \in \mathbb{N}$, berlaku $a^j \equiv a^k \pmod{n}$ jika dan hanya jika $j \equiv k \pmod{\mathrm{ord}_n(a)}$.*

BUKTI. Sekali lagi, satu arah sangat mudah. Misalkan $j, k \in \mathbb{N}$ memenuhi $j \equiv k \pmod{\mathrm{ord}_n(a)}$. Karena kesimpulannya simetris dalam j dan k, tanpa mengurangi keumuman ambil $j \geq k$. Dengan demikian, $\exists \ell \in \mathbb{Z}_{\geq 0}$ sedemikian sehingga $j = k + \mathrm{ord}_n(a) \cdot \ell$, dan

$$a^j = a^{k + \mathrm{ord}_n(a)\cdot \ell} = a^k \cdot (a^{\mathrm{ord}_n(a)})^\ell \equiv a^k \cdot 1^\ell = a^k \pmod{n}\,.$$

Sebaliknya, misalkan $j, k \in \mathbb{N}$ memenuhi $a^j \equiv a^k \pmod{n}$. Jika $j = k$, kesimpulannya langsung berlaku. Jika $j \neq k$, tanpa mengurangi keumuman ambil $j > k$, sehingga $j - k \in \mathbb{N}$. Kalikan kedua ruas kongruensi dengan $(a^{-1})^k$, yang ada karena $\gcd(a, n) = 1$. Kita memperoleh $a^{j-k} \equiv 1 \pmod{n}$. Menurut Teorema 5.1.1, $\mathrm{ord}_n(a) \mid (j - k)$, atau dengan kata lain $j \equiv k \pmod{\mathrm{ord}_n(a)}$. □

CONTOH 5.1.3. Baris-baris pada Tabel 5.0.1 memperlihatkan Teorema 5.1.1 dan 5.1.2: banyaknya unsur dalam setiap subgrup siklik (baris) membagi nilai $\phi(n)$ yang bersesuaian, dan pangkat pembangkit a hanya ditentukan modulo $\mathrm{ord}_n(a)$.

Tampaknya, beberapa subgrup siklik yang lebih kecil juga kadang-kadang muncul sebagai himpunan bagian dari subgrup siklik yang lebih besar. Jadi, modulo $n = 7$, jika $a = 3$ dan $b = a^2 \equiv 2$, kita mempunyai inklusi $\langle b \rangle \subset \langle a \rangle$. Di sini, $\langle b \rangle$ terdiri atas separuh unsur $\langle a \rangle$, yaitu pangkat-pangkat genap dari a:

$$\langle b \rangle = \{b,\ b^2,\ b^3\} = \{2,\ 4,\ 1\} = \{3^2,\ 3^4,\ 3^6\} \subset \{3,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\ 3^6\} = \langle a \rangle$$

Jika kita beralih ke $c = 3^3 \equiv 6$, tetap berlaku $\langle c\rangle \subset \langle a\rangle$, tetapi sekarang $\langle c\rangle$ terdiri atas sepertiga unsur $\langle a\rangle$, yakni pangkat-pangkat a yang merupakan kelipatan 3:

$$\langle c\rangle = \left\{c,\ c^2\right\} = \{6,\ 1\} = \left\{3^3,\ 3^6\right\} \subset \left\{3,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\ 3^6\right\} = \langle a\rangle$$

Bagian terakhir contoh ini mengisyaratkan suatu pernyataan umum: seberapa besar himpunan bagian dari subgrup siklik $\langle a\rangle$ yang dibentuk oleh subgrup siklik $\left\langle a^k\right\rangle$ untuk suatu $k \in \mathbb{N}$? Ukurannya adalah orde unsur a^k tersebut, sehingga kita memerlukan teorema berikut.

TEOREMA 5.1.4. *Misalkan* $n \in \mathbb{N}$ *dan* $a \in \mathbb{Z}$ *memenuhi* $n \geq 2$ *dan* $\gcd(a, n) = 1$. *Maka,* $\forall k \in \mathbb{N}$, $\operatorname{ord}_n(a^k) = \dfrac{\operatorname{ord}_n(a)}{\gcd(\operatorname{ord}_n(a), k)}$.

BUKTI. Tetapkan suatu $k \in \mathbb{N}$, lalu tuliskan $r = \operatorname{ord}_n(a^k)$ dan $s = \operatorname{ord}_n(a)$. Dengan notasi ini, kita hendak membuktikan bahwa $r = \dfrac{s}{\gcd(s, k)}$.

Dalam bukti ini kita akan berulang kali menggunakan fakta bahwa, karena $\gcd$ merupakan pembagi, $\gcd(s, k) \mid s$ dan $\gcd(s, k) \mid k$. Oleh sebab itu, $\dfrac{s}{\gcd(s,k)}, \dfrac{k}{\gcd(s,k)} \in \mathbb{N}$.

Sekarang kita mulai pembuktiannya.

Menurut definisi orde, r adalah bilangan asli terkecil yang memenuhi $(a^k)^r \equiv 1 \pmod{n}$. Perhatikan bahwa

$$(a^k)^{\frac{s}{\gcd(s,k)}} = (a^s)^{\frac{k}{\gcd(s,k)}} \equiv 1^{\frac{k}{\gcd(s,k)}} = 1 \pmod{n}.$$

Menurut Teorema 5.1.1, kita menyimpulkan bahwa $r \;\Big|\; \left(\dfrac{s}{\gcd(s,k)}\right)$.

Terlepas dari sifat minimalnya, karena $a^{kr} = (a^k)^r \equiv 1 \pmod{n}$, Teorema 5.1.1 memberikan $s \mid kr$. Jadi, $\exists m \in \mathbb{N}$ sedemikian sehingga $ms = kr$. Dengan membagi kedua ruas oleh $\gcd(s, k)$, kita memperoleh persamaan bilangan asli

$$m\left(\frac{s}{\gcd(s,k)}\right) = \left(\frac{k}{\gcd(s,k)}\right) r;$$

yang berarti

$$\frac{s}{\gcd(s,k)} \;\Big|\; \left(\frac{k}{\gcd(s,k)}\right) r\ .$$

Menurut Teorema 1.5.5, $\gcd\left(\dfrac{s}{\gcd(s,k)}, \dfrac{k}{\gcd(s,k)}\right) = 1$, maka Lemma Euklides 2.1.6 menyatakan bahwa $\dfrac{s}{\gcd(s,k)} \;\Big|\; r$.

Kita telah menunjukkan bahwa r dan $\dfrac{s}{\gcd(s,k)}$ saling membagi. Dengan demikian, keduanya sama, seperti yang hendak dibuktikan. □

Latihan untuk §5.1.

LATIHAN 5.1.1. Misalkan $n \in \mathbb{N}$ memenuhi $n \geq 2$. Buktikan bahwa jika terdapat $a \in (\mathbb{Z}/n\mathbb{Z})^*$ sedemikian sehingga $\mathrm{ord}_n(a) = n - 1$, maka n prima.

LATIHAN 5.1.2. Misalkan p adalah bilangan prima ganjil dan $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Buktikan bahwa jika $\exists k \in \mathbb{N}$ sedemikian sehingga $\mathrm{ord}_p(a) = 2k$, maka $a^k \equiv -1 \pmod{p}$. *[Petunjuk: lihat bukti Lemma 3.2.1.]*

LATIHAN 5.1.3. Misalkan $n \in \mathbb{N}$ memenuhi $n \geq 2$ dan $a, b \in \mathbb{Z}$ memenuhi $\gcd(a, n) = \gcd(b, n) = 1$. Buktikan bahwa

$$\mathrm{ord}_n(ab) \mid \mathrm{ord}_n(a)\,\mathrm{ord}_n(b)\,.$$

LATIHAN 5.1.4. Buktikan, dengan melengkapi perincian kerangka berikut, bahwa terdapat tak berhingga banyak bilangan prima yang kongruen dengan 1 modulo 4:

(1) Buktikan: jika bilangan prima ganjil p dan $n \in \mathbb{Z}$ memenuhi $n^2 \equiv -1 \pmod{p}$, maka $4 \mid \phi(p)$ *[gunakan sebuah teorema dalam bagian ini]*. Mengapa bilangan prima genap harus dikecualikan di sini?
(2) Jadi, untuk $n \in \mathbb{Z}$, setiap pembagi prima ganjil dari $n^2 + 1$ kongruen dengan 1 modulo 4.
(3) Sekarang, andaikan demi memperoleh kontradiksi bahwa hanya terdapat berhingga banyak bilangan prima $p_1, \ldots, p_n$ yang kongruen dengan 1 modulo 4, lalu tinjau bilangan $(2p_1 \cdot \cdots \cdot p_n)^2 + 1$. Terapkan langkah sebelumnya ....

5.2. Selingan yang Diperlukan: Teorema Gauss tentang Jumlah Nilai Fungsi Phi Euler

Kelak dalam bab ini, kita akan memerlukan sebuah fakta tentang fungsi ϕ Euler yang pertama kali dibuktikan oleh Gauss:

TEOREMA 5.2.1. *Untuk setiap* $n \in \mathbb{N}$, $\displaystyle\sum_{\substack{d\in\mathbb{N}\\ d|n}} \phi(d) = n$.

Kita akan memberikan dua bukti yang menyoroti aspek berbeda dari identitas ini:

BUKTI 1. Tetapkan $n \in \mathbb{N}$.

Untuk setiap pilihan pembagi positif $d \mid n$, definisikan himpunan bagian dari $\{1, \ldots, n\}$ berikut:

$$S_d = \{k \in \mathbb{N} \mid 1 \leq k \leq n \text{ dan } \gcd(k, n) = d\} \ .$$

Himpunan-himpunan ini saling lepas. Memang, untuk setiap $k \in \mathbb{N}$ dengan $1 \leq k \leq n$, nilai $d = \gcd(k, n)$ sudah tertentu, sehingga k hanya berada dalam S_d tersebut.

Untuk $k \in S_d$, berlaku $\gcd(k, n) = d$. Menurut Teorema 1.5.5, $\gcd(k/d, n/d) = 1$. Jadi, $\#(S_d)$ adalah banyaknya unsur $\ell \in \mathbb{N}$ dalam rentang $1 \leq \ell \leq n/d$ yang relatif prima terhadap n/d; dengan kata lain, $\#(S_d) = \phi(n/d)$.

Setiap $k \in \mathbb{Z}$ dalam rentang $1 \leq k \leq n$ berada tepat dalam satu S_d semacam ini, dengan d suatu pembagi positif dari n. Oleh karena itu,

$$\{1, \ldots, n\} = \bigcup_{\substack{d\in\mathbb{N}\\ d|n}} S_d$$

sehingga

$$n = \#\left(\{1, \ldots, n\}\right) = \#\left(\bigcup_{\substack{d\in\mathbb{N}\\ d|n}} S_d\right) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} \#\left(S_d\right) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} \phi(n/d) \ .$$

Namun, ketika d merentang seluruh pembagi positif n, demikian pula n/d. Dengan kata lain,

$$\{d \mid d \in \mathbb{N},\ 1 \leq d \leq n \text{ dan } d \mid n\} = \{n/d \mid d \in \mathbb{N},\ 1 \leq d \leq n \text{ dan } d \mid n\}$$

Karena itu, persamaan besar terakhir dapat ditulis ulang sebagai

$$n = \sum_{\substack{d\in\mathbb{N}\\ d|n}} \phi(n/d) = \sum_{\substack{d\in\mathbb{N}\\ d|n}} \phi(d)$$

seperti yang hendak dibuktikan. □

BUKTI 2. Pendekatan ini berpusat pada fungsi

$$F(n) = \sum_{\substack{d \in \mathbb{N} \\ d|n}} \phi(d) \ ,$$

yang mempunyai beberapa sifat sangat baik.

Sebagai contoh, misalkan p prima dan $k \in \mathbb{N}$. Pembagi-pembagi p^k adalah $1, p, p^2, \ldots, p^k$, sehingga

$$F(p^k) = \phi(1)+\phi(p)+\phi(p^2)+\cdots+\phi(p^k) = 1+(p-1)+(p^2-p)+\cdots+(p^k-p^{k-1}) = p^k \ .$$

Selanjutnya, jika p dan q adalah bilangan prima berbeda, pembagi-pembagi pq adalah 1, p, q, dan pq. Selain itu, $\gcd(p, q) = 1$. Jadi, menurut Teorema 2.5.3,

$$\begin{aligned} F(pq) &= \phi(1) + \phi(p) + \phi(q) + \phi(pq) \\ &= \phi(1) + \phi(p) + \phi(q) + \phi(p)\phi(q) \\ &= (1 + \phi(p))(1 + \phi(q)) \\ &= F(p)F(q) \ . \end{aligned}$$

Dari fakta ini, dapat dibuktikan (sebagai latihan di bawah) bahwa $F(ab) = F(a)F(b)$ setiap kali $a, b \in \mathbb{N}$ relatif prima. Artinya, F mempunyai sifat multiplikatif terhadap faktor-faktor yang relatif prima, sama seperti ϕ.

Sekarang kita siap menyelesaikan bukti. Ambil sebarang $n \in \mathbb{N}$ dengan $n > 1$ (untuk $n = 1$, teorema ini langsung benar). Misalkan faktorisasi prima dari n diberikan oleh

$$n = p_1^{k_1} \cdot \cdots \cdot p_r^{k_r} \ ,$$

dengan $\{p_1, \ldots, p_r\}$ bilangan-bilangan prima yang berbeda. Karena itu, $\gcd(p_i^{k_i}, p_j^{k_j}) = 1$ jika $i \neq j$. Dengan memakai sifat multiplikatif F dan perhitungan F untuk pangkat-pangkat bilangan prima, kita menyimpulkan

$$\begin{aligned} F(n) &= F(p_1^{k_1} \cdot \cdots \cdot p_r^{k_r}) \\ &= F(p_1^{k_1}) \cdot \cdots \cdot F(p_r^{k_r}) \\ &= p_1^{k_1} \cdot \cdots \cdot p_r^{k_r} \\ &= n \ , \end{aligned}$$

seperti yang hendak dibuktikan. □

Latihan untuk §5.2.

LATIHAN 5.2.1. Selesaikan bukti kedua Teorema Gauss 5.2.1 dengan membuktikan bahwa $F(ab) = F(a)F(b)$ untuk setiap $a, b \in \mathbb{N}$ yang relatif prima.

5.3. Akar Primitif

Sekarang kita kembali ke unsur-unsur yang membangkitkan subgrup siklik besar. Unsur-unsur tersebut mempunyai nama khusus:

DEFINISI 5.3.1. Untuk $n \in \mathbb{N}$ dengan $n \geq 2$, unsur $a \in (\mathbb{Z}/n\mathbb{Z})^*$ disebut **akar primitif modulo** n jika $\mathrm{ord}_n(a) = \phi(n)$. Kita juga menyebut bilangan bulat $x \in \mathbb{Z}$ sebagai **akar primitif modulo** n jika $[x]_n$ merupakan akar primitif dalam pengertian yang baru saja didefinisikan.

CONTOH 5.3.2. Dari kedua tabel dalam pendahuluan bab ini, kita dapat membaca akar-akar primitif berikut untuk setiap modulus n:

n	Akar primitif modulo n	$\phi(n)$	$\phi(\phi(n))$
2	1	1	1
3	2	2	1
4	3	2	1
5	2, 3	4	2
6	5	2	1
7	3, 5	6	2
8	*tidak ada*	4	2
⋮			
16	*tidak ada*	8	4
17	3, 5, 6, 7, 10, 11, 12, 14	16	8

TABEL 5.3.1. Akar primitif untuk $n = 2, \ldots, 8, 16, 17$

Kita menyertakan kolom $\phi(n)$ karena setiap akar primitif harus mempunyai orde tersebut. Kita juga menambahkan kolom $\phi(\phi(n))$ karena, seolah-olah melalui suatu keajaiban, nilai itu sering menghitung banyaknya akar primitif.

Mari kita nyatakan secara formal dan buktikan hasil umum yang tampak dalam contoh ini:

TEOREMA 5.3.3. *Untuk $n \in \mathbb{N}$ dengan $n \geq 2$, jika n mempunyai akar primitif, maka n mempunyai tepat $\phi(\phi(n))$ akar primitif.*

BUKTI. Misalkan $a \in (\mathbb{Z}/n\mathbb{Z})^*$ suatu akar primitif. Artinya,

$$\langle a \rangle = \left\{a,\ a^2,\ \ldots\ a^{\mathrm{ord}_n(a)}\right\} = (\mathbb{Z}/n\mathbb{Z})^*$$

karena $\mathrm{ord}_n(a) = \phi(n) = \#\left((\mathbb{Z}/n\mathbb{Z})^*\right)$. Setiap akar primitif lain b, sebagai unsur $(\mathbb{Z}/n\mathbb{Z})^*$, harus merupakan salah satu pangkat a tersebut. Dengan memilih wakil pangkat secara unik, terdapat tepat satu k dengan $1 \leq k \leq \phi(n)$ sedemikian sehingga $b = a^k$.

Agar b ini menjadi akar primitif, ordenya harus $\phi(n)$. Namun, menurut Teorema 5.1.4,

$$\mathrm{ord}_n(b) = \frac{\mathrm{ord}_n(a)}{\gcd(\mathrm{ord}_n(a), k)} = \frac{\phi(n)}{\gcd(\phi(n), k)} .$$

Jadi, $b = a^k$ merupakan akar primitif jika dan hanya jika $\gcd(\phi(n), k) = 1$. Menurut definisi fungsi ϕ Euler , di antara $1 \leq k \leq \phi(n)$ terdapat tepat $\phi(\phi(n))$ nilai k semacam itu. □

Mari kita lihat apakah, dalam keadaan tertentu, kita dapat membuktikan keberadaan akar primitif yang menjadi syarat awal teorema di atas. Keadaan termudah tampaknya terjadi ketika modulusnya prima, sebab dalam kasus itu kita mempunyai perangkat yang paling kuat.

Mencari unsur dengan orde tertentu d antara lain berarti mencari solusi persamaan $x^d - 1 \equiv 0 \pmod{p}$. Langkah pertamanya ialah teorema Lagrange berikut yang lebih umum mengenai polinomial modulo p:

TEOREMA 5.3.4. *Untuk $n \in \mathbb{N}$ dan $a_0, \ldots, a_n \in \mathbb{Z}$, polinomial*

$$a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p} ,$$

dengan $a_n \not\equiv 0 \pmod{p}$ mempunyai paling banyak n solusi dalam $\mathbb{Z}/p\mathbb{Z}$ jika p prima.

BUKTI. Kita menggunakan induksi pada derajat n. Kasus dasar $n = 1$ berarti menyelesaikan kongruensi linear $a_1 x + a_0 \equiv 0 \pmod{p}$ dengan $a_1 \not\equiv 0 \pmod{p}$. Karena p prima, hal ini berarti $\gcd(p, a_1) = 1$. Jadi, menurut versi Teorema 2.2.4 yang dinyatakan dalam Catatan 2.2.5, kongruensi linear tersebut mempunyai solusi unik modulo p.

Untuk langkah induksi, andaikan teorema benar untuk suatu $n \in \mathbb{N}$, lalu kita buktikan kasus $n + 1$. Misalkan $a_0, \ldots, a_{n+1} \in \mathbb{Z}$ memenuhi $a_{n+1} \not\equiv 0 \pmod{p}$. Jika

$$a(x) = a_{n+1} x^{n+1} + a_n x^n + \cdots + a_1 x + a_0$$

tidak mempunyai akar modulo p, teorema jelas benar untuk polinomial berderajat $n+1$ ini: banyaknya solusi $a(x) \equiv 0 \pmod{p}$ adalah $0 < n + 1$.

Sebaliknya, jika $a(x)$ mempunyai sekurang-kurangnya satu akar modulo p, pilih wakil bilangan bulatnya z_1. Pembagian panjang polinomial memberikan

$$a(x) = b(x)(x - z_1) + r(x)$$

dengan $b(x)$ dan $r(x)$ polinomial berkoefisien bilangan bulat yang memenuhi

$$0 \leq \deg(r(x)) < \deg(x - z_1) = 1 .$$

Karena itu, $r(x)$ merupakan polinomial konstan, katakanlah bernilai $r_1 \in \mathbb{Z}$.

Substitusikan z_1 ke dalam rumus hasil pembagian polinomial di atas:

$$0 \equiv a(z_1) \equiv b(z_1)(z_1 - z_1) + r_1 \equiv r_1 \pmod{p} .$$

Jadi, $r_1 \equiv 0 \pmod{p}$, sehingga $a(x) \equiv b(x)(x - z_1) \pmod{p}$. Koefisien a_{n+1} sama dengan koefisien utama $b(x)$, sehingga koefisien utama itu tidak kongruen dengan 0 modulo p.

Karena itu, hipotesis induksi berlaku bagi $b(x)$ dan menyatakan bahwa $b(x)$ mempunyai paling banyak n akar modulo p. Akar-akar $b(x)$ tersebut, ditambah satu akar dari $(x - z_1)$, berjumlah paling banyak $n + 1$ akar bagi $a(x) \equiv b(x)(x - z_1) \pmod{p}$.

Untuk menuntaskan bukti, kita hanya perlu memastikan bahwa setiap akar $a(x)$ memang merupakan akar $b(x)$ atau $(x - z_1)$. Misalkan $r \in \mathbb{Z}$ suatu akar. Maka

$$a(r) = b(r)(r - z_1) \equiv 0 \pmod{p},$$

yang berarti $p \mid b(r)(r - z_1)$. Menurut Proposisi 3.1.5, haruslah $p \mid b(r)$ atau $p \mid (r - z_1)$. Dengan kata lain, $b(r) \equiv 0 \pmod{p}$ atau $(r - z_1) \equiv 0 \pmod{p}$, seperti yang diharapkan. [Ini menggunakan apa yang dalam aljabar dasar disebut "sifat hasil kali nol". Sifat tersebut berlaku dalam $\mathbb{Z}/p\mathbb{Z}$ untuk p prima menurut Proposisi 3.1.5; dalam aljabar abstrak, kita mengatakan bahwa $\mathbb{Z}/p\mathbb{Z}$ merupakan suatu *domain* jika p prima.]

Jadi, semua akar $a(x)$ berasal dari akar $b(x)$ atau $(x - z_1)$, sehingga banyaknya paling besar $n + 1$. Langkah induksi pun terbukti. □

Demikianlah batas maksimum banyaknya akar. Dalam kasus khusus berikut, kita dapat menentukan banyaknya akar secara tepat:

TEOREMA 5.3.5. *Jika p prima dan $d \in \mathbb{N}$ memenuhi $d \mid p-1$, maka, hingga kongruensi modulo p, terdapat tepat d solusi bagi kongruensi*

$$x^d = 1 \pmod{p}\,.$$

BUKTI. Misalkan p dan d seperti dalam pernyataan, lalu definisikan $m = (p - 1)/d \in \mathbb{N}$. Kita menggunakan faktorisasi cerdik berikut:

$$\begin{aligned} a(x) &= x^d - 1, \\ b(x) &= x^{dm-d} + x^{dm-2d} + \cdots + x^d + 1, \text{ dan} \\ c(x) &= x^{p-1} - 1 \end{aligned}$$

sehingga $c(x) = a(x)b(x)$.

Menurut Teorema Kecil Fermat, $c(x)$ mempunyai tepat $p - 1$ akar berbeda modulo p, yaitu $\{1, \ldots, p - 1\}$. Selain itu, menurut Teorema 5.3.4, $b(x)$ mempunyai paling banyak $\deg(b(x)) = dm - d = p - 1 - d$ akar. Seperti dalam bukti teorema tersebut (pada bagian tentang "sifat hasil kali nol"), himpunan akar $c(x)$ adalah gabungan himpunan akar $a(x)$ dan $b(x)$. Karena $p - 1$ akar berbeda itu harus tertampung dalam gabungan tersebut, sedangkan $b(x)$ mempunyai paling banyak $p - 1 - d$ akar, $a(x)$ mempunyai sekurang-kurangnya d akar. Di sisi lain, Teorema 5.3.4 membatasi polinomial berderajat d ini pada paling banyak d akar. Jadi, $a(x) = x^d - 1$ mempunyai tepat d akar modulo p. □

Sekarang kita dapat menghitung secara tepat kelas-kelas kongruensi dalam $\mathbb{Z}/p\mathbb{Z}$, untuk p prima, yang mempunyai orde tertentu:

TEOREMA 5.3.6. *Jika p prima dan $d \in \mathbb{N}$ memenuhi $d \mid p-1$, maka terdapat tepat $\phi(d)$ kelas kongruensi berbeda berorde d dalam $\mathbb{Z}/p\mathbb{Z}$.*

BUKTI. Misalkan p dan d seperti dalam pernyataan, lalu tuliskan

$$\psi(k) = \#\left(\{\ell \in \mathbb{Z} \mid 1 \le \ell \le p-1 \text{ dan } \operatorname{ord}_p(\ell) = k\}\right) .$$

Menurut versi Teorema Lagrange kita, Teorema 3.3.3, setiap $\ell \in \mathbb{Z}$ dengan $1 \le \ell \le p-1$ mempunyai orde yang membagi $\phi(p) = p-1$. Jadi,

$$\sum_{\substack{k\in\mathbb{N}\\ k\mid p-1}} \psi(k) = p-1 .$$

Selain itu, menurut Teorema Gauss 5.2.1 ,

$$\sum_{\substack{k\in\mathbb{N}\\ k\mid p-1}} \phi(k) = p-1 .$$

Dengan demikian,

$$\sum_{\substack{k\in\mathbb{N}\\ k\mid p-1}} \phi(k) = \sum_{\substack{k\in\mathbb{N}\\ k\mid p-1}} \psi(k) .$$

Sekarang cukup ditunjukkan bahwa $\psi(k) \le \phi(k)$ untuk setiap $k \in \mathbb{N}$ yang membagi $p-1$. Karena kedua jumlah berhingga di atas sama, ketaksamaan tersebut kemudian harus berupa kesamaan untuk setiap k.

Ambil $k \in \mathbb{N}$ dengan $k \mid p-1$. Jika $\psi(k) = 0$, tidak ada unsur berorde k, dan tentu saja $\psi(k) \le \phi(k)$ karena $\phi(k) > 0$.

Sekarang misalkan $\psi(k) > 0$, sehingga terdapat unsur a berorde k dalam $\mathbb{Z}/p\mathbb{Z}$. Untuk setiap $n \in \mathbb{N}$, $(a^n)^k = (a^k)^n \equiv 1^n \equiv 1 \pmod p$. Jadi, $a, \ldots, a^k$ merupakan k unsur berbeda dalam $\mathbb{Z}/p\mathbb{Z}$ yang semuanya memenuhi

$$x^k - 1 \equiv 0 \pmod p .$$

Menurut Teorema 5.3.5, kongruensi ini mempunyai tepat k solusi. Dengan demikian, $a, \ldots, a^k$ merupakan seluruh solusinya. Di antara solusi tersebut terdapat semua unsur $\mathbb{Z}/p\mathbb{Z}$ yang berorde k , serta mungkin unsur berorde pembagi k.

Teorema 5.1.4 menentukan secara tepat orde unsur-unsur $a, \ldots, a^k$: orde a^ℓ adalah

$$\frac{\operatorname{ord}_p(a)}{\gcd(\operatorname{ord}_p(a), \ell)} = \frac{k}{\gcd(k, \ell)} .$$

Jadi, unsur-unsur $\mathbb{Z}/p\mathbb{Z}$ berorde k adalah tepat unsur a^ℓ dengan $1 \le \ell \le k$ dan $\gcd(k, \ell) = 1$. Banyaknya tepat $\phi(k)$; dengan kata lain, $\psi(k) = \phi(k)$. □

Jadi, inilah kesimpulan utamanya:

AKIBAT 5.3.7. *Jika p prima, terdapat $\phi(p-1)$ akar primitif dalam $\mathbb{Z}/p\mathbb{Z}$.*

BUKTI. Gunakan $d = p-1$ dalam teorema sebelumnya. □

Untuk menuntaskan rangkaian dugaan yang mengawali bab dan bagian ini, mari kita buktikan teorema berikut.

TEOREMA 5.3.8. *Misalkan $k \in \mathbb{N}$ memenuhi $k \geq 3$. Maka 2^k tidak mempunyai akar primitif.*

BUKTI. Kita akan membuktikan dengan induksi pada k bahwa, untuk setiap bilangan ganjil a,

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

Untuk kasus dasar $k = 3$, perhatikan semua kelas kongruensi dalam $\mathbb{Z}/8\mathbb{Z}$ yang mempunyai wakil ganjil beserta kuadrat kelas-kelas tersebut:

$$[1]_8^2 = [1]_8, \qquad [3]_8^2 = [9]_8 = [1]_8, \qquad [5]_8^2 = [25]_8 = [1]_8, \quad \text{dan} \quad [7]_8^2 = [49]_8 = [1]_8 .$$

Jadi, kasus dasar $k = 3$ terbukti.

Sekarang andaikan pernyataan berlaku untuk nilai k, yang berarti bahwa untuk setiap a ganjil,

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} .$$

Dengan kata lain, $\exists \ell \in \mathbb{Z}$ sedemikian sehingga

$$a^{2^{k-2}} = 2^k \ell + 1 .$$

Dengan menguadratkan kedua ruas, kita memperoleh

$$a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2 = \left(2^k \ell + 1\right)^2 = 2^{2k}\ell^2 + 2 \cdot 2^k \ell + 1 = 2^{k+1}\left(2^{k-1}\ell^2 + \ell\right) + 1,$$

yang berarti

$$a^{2^{(k+1)-2}} = a^{2^{k-1}} \equiv 1 \pmod{2^{(k+1)}} .$$

Dengan demikian, bukti induktif bagi pernyataan awal selesai. Perhatikan bahwa untuk setiap a ganjil, atau dengan kata lain setiap $a \in (\mathbb{Z}/2^k\mathbb{Z})^*$, Teorema 5.1.1 memberikan $\operatorname{ord}_{2^k}(a) \mid 2^{k-2}$, sehingga $\operatorname{ord}_{2^k}(a) \leq 2^{k-2} < 2^{k-1}$. Jadi, 2^k tidak mempunyai akar primitif: akar semacam itu harus berupa bilangan ganjil berorde $\phi(2^k) = 2^{k-1}$. □

Seperti yang tampak dari beberapa contoh yang telah kita hitung, pangkat besar dari dua tidak mempunyai akar primitif.

Latihan untuk §5.3.

LATIHAN 5.3.1. Nyatakan setiap akar primitif modulo 17 sebagai pangkat dari salah satunya.

LATIHAN 5.3.2. Temukan semua akar primitif untuk bilangan prima 11 dan 13, lalu nyatakan masing-masing sebagai pangkat dari salah satu akar primitifnya.

LATIHAN 5.3.3. Untuk setiap orde yang mungkin, temukan semua unsur $\mathbb{Z}/13\mathbb{Z}$ yang mempunyai orde tersebut.

LATIHAN 5.3.4. Dengan menyatakan semuanya sebagai pangkat dari satu akar primitif, gunakan Akibat 5.3.7 untuk membuktikan satu arah Teorema Wilson.

LATIHAN 5.3.5. Jika r merupakan akar primitif dari bilangan prima ganjil p, buktikan bahwa $r^{(p-1)/2} \equiv -1 \pmod{p}$. Buktikan pula bahwa jika s adalah akar primitif lain dari p, maka rs tidak mungkin merupakan akar primitif.

LATIHAN 5.3.6. Buktikan bahwa invers suatu akar primitif selalu merupakan akar primitif.

LATIHAN 5.3.7. Jika p prima dan kongruen dengan $1 \mod 4$, buktikan bahwa untuk setiap akar primitif r dari p, nilai $-r$ juga merupakan akar primitif. Jika p prima dan kongruen dengan $3 \mod 4$, buktikan bahwa $\mathrm{ord}_p(-r) = (p-1)/2$.

5.4. Indeks

Untuk beberapa nilai $n \in \mathbb{N}$, terdapat akar primitif $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Dalam keadaan itu, kita telah melihat bahwa

$$\langle a \rangle = \left\{ a,\ a^2,\ \ldots\ a^{\mathrm{ord}_n(a)} \right\} = (\mathbb{Z}/n\mathbb{Z})^* \ .$$

Artinya, setiap $b \in (\mathbb{Z}/n\mathbb{Z})^*$ merupakan suatu pangkat dari a. Mungkin Anda bertanya, "Pangkat yang mana?" Untuk menjawabnya, kita membuat definisi berikut.

DEFINISI 5.4.1. Jika $n \in \mathbb{N}$ mempunyai akar primitif a, maka untuk setiap $b \in \mathbb{Z}$ dengan $\gcd(b, n) = 1$, bilangan terkecil $k \in \mathbb{N}$ yang memenuhi $b \equiv a^k \pmod{n}$ disebut **indeks** b **relatif terhadap** a dan dinotasikan dengan $\mathrm{ind}_a(b)$.

Kita kadang-kadang juga membahas $\mathrm{ind}_a(x)$ untuk $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Maksudnya ialah indeks relatif terhadap a dari sebarang wakil b bagi kelas kongruensi x.

CONTOH 5.4.2. Berdasarkan tabel-tabel di atas (5.0.1, 5.0.2, dan 5.3.1), kita dapat dengan mudah menghitung sejumlah contoh. Pertama, untuk modulus-modulus kecil yang hanya mempunyai sedikit akar primitif:

n	a	b	$\mathrm{ind}_a(b)$
2	1	1	1
3	2	1	2
		2	1
4	3	1	2
		3	1
5	2	1	4
		2	1
		3	3
		4	2
5	3	1	4
		2	3
		3	1
		4	2

n	a	b	$\mathrm{ind}_a(b)$
7	3	1	6
		2	2
		3	1
		4	4
		5	5
		6	3
	5	1	6
		2	4
		3	5
		4	2
		5	1
		6	3

TABEL 5.4.1. Nilai indeks untuk modulus $n = 2,\ 3,\ 4,\ 5,\ 7$

Dari dua modulus lebih besar yang telah kita hitung, hanya $n = 17$ yang mempunyai akar primitif. Karena $(\mathbb{Z}/17\mathbb{Z})^*$ mempunyai 16 unsur dan 8 akar primitif, kita membuat tabel yang lebih besar khusus untuk modulus ini:

$\mathrm{ind}_a(b)$		b															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a	3	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
	5	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8
	6	16	2	15	4	11	1	5	6	14	13	9	3	12	7	10	8
	7	16	10	3	4	15	13	1	14	6	9	5	7	12	11	2	8
	10	16	10	11	4	7	5	9	14	6	1	13	15	12	3	2	8
	11	16	2	7	4	3	9	13	6	14	5	1	11	12	15	10	8
	12	16	6	5	12	9	11	7	2	10	15	3	1	4	13	14	8
	14	16	14	9	12	13	7	3	10	2	11	15	5	4	1	6	8

TABEL 5.4.2. Nilai indeks untuk modulus $n = 17$

Berdasarkan contoh-contoh dan definisi indeks yang sederhana ini, beberapa dugaan muncul secara alami. Banyak di antaranya sangat mudah dibuktikan (dan dijadikan latihan):

TEOREMA 5.4.3. *Misalkan $n \in \mathbb{N}$ mempunyai akar primitif a. Maka*

(1) $\mathrm{ind}_a(1) = \mathrm{ord}_n(a) = \phi(n)$*; secara ekuivalen,* $\mathrm{ind}_a(1) \equiv 0 \pmod{\phi(n)}$*;*

(2) $\mathrm{ind}_a(a) = 1$*;*

(3) *untuk setiap $b, c \in \mathbb{Z}$ yang memenuhi $\gcd(b, n) = \gcd(c, n) = 1$, berlaku*

$$\mathrm{ind}_a(bc) \equiv \mathrm{ind}_a(b) + \mathrm{ind}_a(c) \pmod{\phi(n)}$$

(4) *untuk setiap $b \in \mathbb{Z}$ dengan $\gcd(b, n) = 1$ dan setiap $k \in \mathbb{N}$, berlaku*

$$\mathrm{ind}_a(b^k) \equiv k \cdot \mathrm{ind}_a(b) \pmod{\phi(n)}$$

Sifat-sifat ind_a ini sangat mirip dengan sifat dasar logaritma berbasis a. Karena itu, dalam literatur ilmu komputer, indeks disebut **logaritma diskret**. Untuk aplikasi kriptologi, penting untuk memerhatikan bahwa, pada keluarga parameter besar yang dipilih dengan sesuai, eksponensiasi dalam $(\mathbb{Z}/n\mathbb{Z})^*$ merupakan calon fungsi satu arah yang sangat baik:

- Jika n, a, dan k diberikan, eksponensiasi modular cepat merupakan komputasi layak untuk memperoleh $b = a^k$ modulo n.
- Jika n, a, dan b diberikan dengan parameter dari keluarga semacam itu, belum dikenal algoritme klasik layak yang menemukan $k = \mathrm{ind}_a(b)$ dengan $a^k \equiv b \pmod{n}$.

Dalam bagian-bagian berikutnya, kita akan membahas beberapa protokol kriptologi yang berbasis logaritma diskret.

Sebelum beralih ke kriptologi, kita menjelajahi beberapa penerapan matematis murni dari indeks. Seperti penerapan logaritma dalam aljabar dasar, kegunaan indeks berasal dari

Teorema 5.4.3, yang memungkinkan manipulasi aljabar terhadap pangkat dan perkalian secara mudah. Berikut sebuah contoh.

CONTOH 5.4.4. Kita menggunakan indeks untuk menyelesaikan kongruensi

$$3x^5 \equiv 4 \pmod 7$$

dengan mula-mula mengambil ind_5 pada kedua ruas:

$$\mathrm{ind}_5(3) + 5\,\mathrm{ind}_5(x) \equiv \mathrm{ind}_5(4) \pmod 6$$

dan menerapkan semua aturan dalam Teorema 5.4.3. Dengan melihat Tabel 5.4.1, kita mengubahnya menjadi

$$5 + 5 \cdot \mathrm{ind}_5(x) \equiv 2 \pmod 6$$

atau, setelah diselesaikan,

$$\mathrm{ind}_5(x) \equiv 5^{-1} \cdot 3 \equiv 5 \cdot 3 \equiv 3 \pmod 6$$

yang, setelah kita kembali melihat tabel, berarti $x = 6$.

Sebagai pemeriksaan, perhatikan bahwa $3 \cdot 6^5 = 23328 \equiv 4 \pmod 7$.

Bagaimana jika kita menyelesaikan persamaan yang sama, tetapi memakai akar primitif yang berbeda sebagai basis indeks? Hitung

$$\mathrm{ind}_3(3) + 5\,\mathrm{ind}_3(x) \equiv \mathrm{ind}_3(4) \pmod 6$$

sehingga

$$1 + 5 \cdot \mathrm{ind}_3(x) \equiv 4 \pmod 6$$

dan kita memperoleh persamaan serupa,

$$\mathrm{ind}_3(x) \equiv 5^{-1} \cdot 3 \equiv 3 \pmod 6$$

sehingga solusinya tetap $x = 6$.

Perhatian: Kesalahan umum ketika menggunakan indeks ialah memakai modulus yang sama untuk indeks dan kongruensi asal. Padahal, ketika kongruensi asal adalah modulo n, untuk $n \in \mathbb{N}$, kongruensi indeks adalah modulo $\phi(n)$!

Latihan untuk §5.4.

LATIHAN 5.4.1. Untuk modulus $n = 17$, gunakan indeks untuk menyelesaikan kongruensi berikut:

(a) $4x \equiv 11$ **(b)** $5x^6 \equiv 7$ **(c)** $x^{12} \equiv 13$
(d) $8x^5 \equiv 10$ **(e)** $9x^8 \equiv 8$ **(f)** $7^x \equiv 7$

LATIHAN 5.4.2. Aturan logaritma dalam Teorema 5.4.3 sangat mirip dengan aturan logaritma biasa, tetapi satu aturan belum ada: rumus perubahan basis. Tentukan bentuk rumus tersebut dalam konteks indeks, nyatakan secara formal, lalu buktikan.

LATIHAN 5.4.3. Misalkan p bilangan prima ganjil dan a suatu akar primitif modulo p.

(a) Buktikan bahwa $\mathrm{ind}_a(-1) = (p-1)/2$.
(b) Jika $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$ memenuhi $xy \equiv 1 \pmod{p}$, apa hubungan antara $\mathrm{ind}_a(x)$ dan $\mathrm{ind}_a(y)$? Buktikan!
(c) Jika $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$ memenuhi $x+y \equiv 0 \pmod{p}$, apa hubungan antara $\mathrm{ind}_a(x)$ dan $\mathrm{ind}_a(y)$? Buktikan!

5.5. Pertukaran Kunci Diffie–Hellman

Sekitar setahun sebelum kriptosistem RSA diciptakan, Whitfield Diffie dan Martin Hellman menerbitkan *New directions in cryptography* [**DH76**], uraian lengkap pertama dalam literatur ilmiah terbuka mengenai kriptosistem kunci publik yang dapat berfungsi.[1] Dalam makalah itu mereka mendefinisikan sesuatu yang kemudian dinamai menurut keduanya:

DEFINISI 5.5.1. Protokol berikut disebut **pertukaran kunci Diffie–Hellman** [**DHKE**]:

(1) Alice dan Bob menyepakati sebuah bilangan prima besar p beserta akar primitif $r \in (\mathbb{Z}/p\mathbb{Z})^*$, lalu mengumumkan keduanya.
(2) Alice memilih $\alpha \in \mathbb{Z}$ yang memenuhi $2 \leq \alpha \leq p-2$, menghitung $A = r^\alpha \pmod p$, merahasiakan α, tetapi mengumumkan A.
(3) Bob memilih $\beta \in \mathbb{Z}$ yang memenuhi $2 \leq \beta \leq p-2$, menghitung $B = r^\beta \pmod p$, merahasiakan β, dan mengumumkan B.
(4) Alice memperoleh nilai publik B dan menghitung $S = B^\alpha \pmod p$.
(5) Bob memperoleh A dan menghitung nilai yang sama, $S = A^\beta \pmod p$.
(6) Alice dan Bob memakai rahasia bersama S sebagai kunci untuk komunikasi selanjutnya, yang dienkripsi dengan suatu kriptosistem simetris yang telah mereka sepakati sebelumnya.

Nilai S yang dimiliki Alice dan Bob [tetapi tidak dimiliki Eve] disebut **kunci bersama** atau **rahasia bersama** mereka.

Gambaran grafisnya sebagai berikut:

Pertukaran kunci Diffie–Hellman:

Alice	di jaringan publik	Bob
	pilih bilangan prima p temukan akar primitif r	
pilih α, hitung $A = r^\alpha \pmod p$ umumkan A	$\rightarrowtail A$ $\quad$ $B \leftarrowtail$	pilih β, hitung $B = r^\beta \pmod p$ umumkan B
peroleh B, hitung $S = B^\alpha \pmod p$		peroleh A, hitung $S = A^\beta \pmod p$
kriptografi simetris dengan kunci S $\longleftrightarrow$		

[1] Sebenarnya, beberapa bentuk kriptografi kunci publik yang dapat berfungsi telah ditemukan lebih dahulu di lingkungan intelijen AS dan Britania Raya, tetapi tidak dibagikan kepada publik. Sejak masa awal Perang Dingin, sejumlah pemerintahan besar telah merahasiakan teorema dan bukti matematika.

PROPOSISI 5.5.2. *Jika Alice dan Bob mengikuti protokol DHKE, keduanya menghitung kunci bersama yang sama;* dengan kata lain, DHKE berfungsi.

BUKTI. Hanya sedikit yang perlu diperiksa. Dengan memakai notasi dalam definisi dan, tepat di tengah, sifat komutatif perkalian, kita memperoleh

$$B^\alpha \equiv \left(r^\beta\right)^\alpha \equiv r^{\beta\cdot\alpha} \equiv r^{\alpha\cdot\beta} \equiv \left(r^\alpha\right)^\beta \equiv A^\beta \pmod{p}\,.$$

Ujung kiri kongruensi ini adalah S yang dihitung Alice, sedangkan ujung kanannya adalah S yang dihitung Bob; keduanya sama sebagai kelas modulo p. □

CONTOH 5.5.3. Dalam pembicaraan terbuka, Alice dan Bob sepakat memakai bilangan prima $p = 617$ beserta akar primitifnya $r = 17$.

Alice secara privat memilih nilai rahasianya $\alpha = 19$ dan mengirim nilai

$$A = 17^{19} \equiv 385 \pmod{617}$$

kepada Bob melalui surel yang tidak aman. (Tentu saja, setiap surel tanpa enkripsi tidak aman.)

Bob memilih nilai rahasianya $\beta = 13$ dan mengirim nilai

$$B = 17^{13} \equiv 227 \pmod{617}$$

kepada Alice melalui surel yang tidak aman.

Alice menghitung rahasia bersama

$$S = B^\alpha = 227^{19} \equiv 127 \pmod{617}\,.$$

Bob menghitung rahasia bersama yang sama melalui

$$S = A^\beta = 385^{13} \equiv 127 \pmod{617}\,.$$

Mereka kemudian dapat memakai nilai ini sebagai kunci kriptografi simetris untuk sisa komunikasi tersebut.

Bagaimana dengan kepraktisan DHKE? Seperti dibahas dalam §4.4, mencari bilangan prima [besar] p (kita tetap memakai notasi dari Definisi 5.5.1) layak secara komputasi, demikian pula beberapa eksponensiasi modular dalam protokol DHKE. Masih tersisa persoalan mencari akar primitif r.

Salah satu caranya ialah menghindari pencarian r lebih dari sekali. Setelah satu bilangan prima p beserta akar primitif r modulo p ditemukan, setiap pengguna dapat memilih rahasianya sendiri (α milik Alice dan β milik Bob) tanpa tumpang tindih atau konflik. Pendekatan ini disarankan dalam sejumlah standar Internet; lihat, *misalnya,* [**HC**] dan [**LK08**].

Strategi lain yang lebih matematis didasarkan pada definisi berikut. Kita menyertakannya karena konsep ini menarik secara matematis dan tokoh yang namanya diabadikan di dalamnya menjalani kehidupan yang luar biasa.

DEFINISI 5.5.4. Bilangan prima p yang membuat $2p + 1$ juga prima disebut **prima Sophie Germain**.

Belum diketahui berapa banyak prima Sophie Germain yang ada, meskipun diduga jumlahnya tak hingga. Bahkan, terdapat dugaan yang cermat mengenai kepadatan asimtotik prima semacam itu serta teknik algoritmik untuk membangkitkannya secara efisien; lihat [**Sho09**].

CONTOH 5.5.5. Tujuh belas prima Sophie Germain pertama ialah

$$2,\ 3,\ 5,\ 11,\ 23,\ 29,\ 41,\ 53,\ 83,\ 89,\ 113,\ 131,\ 173,\ 179,\ 191,\ 233,\ 239$$

Barisan semua prima Sophie Germain adalah barisan *A005384* dalam *On-Line Encyclopedia of Integer Sequences*, `oeis.org`.

Pada saat naskah sumber ini ditulis, prima Sophie Germain terbesar yang diketahui ialah

$$18543637900515 \times 2^{666667} - 1$$

yang ditemukan pada 2012 oleh Philipp Bliedung dan sebuah jaringan besar komputer terdistribusi.

Kegunaan prima Sophie Germain dalam DHKE diselidiki pembaca melalui latihan di bawah ini.

Seperti disebutkan dalam bagian sebelumnya 5.4, keamanan DHKE pada keluarga parameter besar yang dipilih dengan sesuai bergantung pada asumsi bahwa eksponensiasi modular berperilaku sebagai fungsi satu arah: layak dihitung ke arah maju (dengan eksponensiasi modular cepat), tetapi belum dikenal cara klasik yang layak untuk membalik operasi itu (yakni menghitung suatu indeks).

Jika logaritma diskret dapat dihitung dengan algoritme layak, Eve dapat membobol DHKE sepenuhnya. Berawal dari nilai publik A dan B, ia akan menghitung $\alpha = \operatorname{ind}_r(A)$ dan $\beta = \operatorname{ind}_r(B)$. Selanjutnya ia dapat menghitung S sebagai B^α, A^β, atau langsung sebagai $r^{\alpha\cdot\beta}$. Setelah memperoleh S, ia dapat mendekripsi komunikasi Alice dan Bob yang lewat.

Sebenarnya, Eve tidak harus mampu menghitung logaritma diskret selama ia dapat menyelesaikan suatu masalah komputasi tertentu.

DEFINISI 5.5.6. **Masalah Diffie–Hellman** [**DHP**] adalah pertanyaan berikut. Diberikan

- bilangan prima p,
- akar primitif $r \in (\mathbb{Z}/p\mathbb{Z})^*$, dan
- dua unsur $a, b \in (\mathbb{Z}/p\mathbb{Z})^*$ yang diketahui berbentuk $a = r^x$ dan $b = r^y$ untuk $x, y \in \mathbb{N}$, meskipun x dan y tidak diketahui,

hitung

- r^{xy} .

Cara efisien untuk menghitung logaritma diskret tentu menghasilkan penyelesaian DHP. Namun, belum diketahui apakah DHP dapat diselesaikan tanpa algoritme lengkap untuk menghitung logaritma diskret. Karena pertanyaan ini masih terbuka pada saat naskah sumber ditulis, pernyataan yang paling cermat ialah bahwa membobol DHKE berarti menyelesaikan DHP. Untuk keluarga parameter besar yang dipilih dengan sesuai, tidak dikenal algoritme klasik yang layak untuk melakukannya.[2]

DHKE merupakan salah satu protokol kriptologi yang paling luas digunakan di Internet. Protokol ini atau variannya dipakai, antara lain, dalam SSL, TLS, SSH, IPsec, dan banyak VPN.

[2]Seperti pada faktorisasi, terdapat algoritme yang diketahui untuk *komputer kuantum* yang menyelesaikan DHP secara efisien; lihat [**Sho94**].

Latihan untuk §5.5.

LATIHAN 5.5.1. Andaikan Anda mempunyai algoritme efisien untuk membangkitkan prima Sophie Germain yang besar. Jelaskan cara memakainya untuk memilih parameter publik awal DHKE: telusuri semua tahap penyiapan protokol ini dan jelaskan bagaimana setiap tahap dapat dilakukan *secara layak*, berdasarkan pembahasan terdahulu tentang perhitungan yang dapat kita lakukan secara layak atau berdasarkan gagasan baru yang Anda kembangkan di sini.

LATIHAN 5.5.2. Bilangan $p = 11717$ adalah prima dan $r = 103$ merupakan akar primitif modulo p. Dengan berperan sebagai Alice, pengajar Anda telah menghitung $A = 5123$.

Berperanlah sebagai Bob dan lakukan apa yang diperlukan untuk membentuk kunci bersama dengan pengajar Anda: hitung S seperti dalam DHKE dan kirimkan B Anda melalui surel agar pengajar juga dapat menghitung S. Kemudian tunggu petunjuk lanjutan melalui surel balasan yang dienkripsi dengan rahasia bersama.

Anda mungkin perlu melakukan perhitungan yang sulit dikerjakan dengan kalkulator genggam. Jika Anda memiliki akses ke dan terbiasa dengan sistem komputer seperti `Octave, Matlab`, atau `Mathematica`, perhitungan ini dapat dilakukan dengan sistem tersebut. Jika tidak, cobalah mencari frasa "fast modular exponentiation applet" dengan mesin pencari favorit Anda atau memakai `wolframalpha.com`.

LATIHAN 5.5.3. Uraikan dengan perincian matematis yang cermat semua langkah yang digunakan dalam serangan man-in-the-middle terhadap DHKE.

5.6. Kriptosistem ElGamal

Seperti disebutkan dalam bagian sebelumnya, untuk keluarga parameter besar yang dipilih dengan sesuai, eksponensiasi modulo bilangan prima publik p merupakan calon fungsi satu arah yang baik. Perhitungan ke arah maju berlangsung cepat (layak), sedangkan inversnya, yakni logaritma diskret relatif terhadap akar primitif r modulo p, belum diketahui dapat dihitung dengan algoritme klasik yang layak—bahkan ketika akar itu diketahui publik. Asumsi ini mendasari DHKE; kini kita membahas cara memakai gagasan satu arah tersebut untuk membentuk kriptosistem kunci publik yang lebih lazim, yaitu kriptosistem ElGamal.

Dalam kriptosistem kunci publik RSA, enkripsi dilakukan dengan eksponensiasi modulo $n = pq$. Dekripsi kemudian dilakukan dengan eksponen yang merupakan invers multiplikatif eksponen enkripsi modulo $\phi(n)$. Pemilik kunci privat, yang mengetahui faktor rahasia p dan q, juga dapat mengetahui eksponen dekripsi karena ia dapat menghitung $\phi(n)$.

Dengan cara serupa, ElGamal memakai operasi aritmetika elementer—mengalikan bentuk numerik pesan dengan suatu faktor pengacak modulo bilangan tertentu— untuk melakukan pengacakan yang diperlukan dalam enkripsi. Cipherteks membawa informasi secukupnya agar penerima yang dituju, yang mengetahui nilai logaritma diskret tertentu, dapat membatalkan perkalian pengacak itu. Berikut rinciannya. Konstruksi buku teks ini menetapkan cara kerja dan kebenaran fungsionalnya; jaminan keamanan yang lebih kuat memerlukan asumsi mengenai grup, pembangkitan parameter, enkode, dan keacakan baru yang independen yang tidak dibuktikan di sini.

DEFINISI 5.6.1. Untuk memulai, Alice memilih bilangan prima besar p, akar primitif r modulo p, dan nilai rahasia $\alpha \in \mathbb{N}$ yang memenuhi $2 \leq \alpha \leq p-2$. Ia menghitung $a = r^\alpha \pmod p$, lalu memasang **kunci publik** [**enkripsi**] **ElGamal** miliknya, yaitu (p, r, a), di situs webnya.

Kunci privat [**dekripsi**] **ElGamal** milik Alice adalah (p, r, α). Hubungan kunci dekripsi dengan kunci enkripsi diberikan oleh $\mathcal{E} : (p, r, \alpha) \mapsto (p, r, r^\alpha \pmod p)$.

Ruang pesannya ialah $\mathcal{M} = \{m \in \mathbb{Z} \mid 2 \leq m \leq p-1\}$. Kita menganggap setiap unsurnya dapat ditafsirkan sebagai pesan bermakna yang dienkode secara numerik dengan suatu skema yang dikenal luas.

Misalkan Bob ingin mengirim plainteks $m \in \mathcal{M}$ kepada Alice. Untuk setiap pesan baru m, ia membangkitkan bilangan acak baru $\beta \in \mathbb{N}$ yang memenuhi $2 \leq \beta \leq p-2$, lalu membentuk cipherteks untuk **enkripsi ElGamal**, yang terdiri atas dua komponen

$$c = e_{(p,r,a)}(m) = (r^\beta \pmod p,\ m \cdot a^\beta \pmod p)\ .$$

Ketika menerima cipherteks $c = (c_1, c_2)$, Alice dapat memulihkan plainteks dengan **dekripsi ElGamal**

$$d_{(p,r,\alpha)}(c_1, c_2) = c_2 \cdot c_1^{p-1-\alpha} \pmod{p} .$$

Semua komponen di atas bersama-sama membentuk **kriptosistem ElGamal**.

Pertama-tama, kita perlu memastikan bahwa konstruksi ini benar dalam arti berikut.

PROPOSISI 5.6.2. *Dengan notasi dalam Definisi 5.6.1, berlaku*

$$d_{(p,r,\alpha)}(e_{(p,r,a)}(m)) = m \quad \forall m \in \mathcal{M} .$$

BUKTI. Cukup lakukan perhitungan berikut:

$$\begin{aligned} d_{(p,r,\alpha)}(e_{(p,r,a)}(m)) &\equiv m \cdot a^\beta \cdot (r^\beta)^{p-1-\alpha} \pmod{p} \\ &\equiv m \cdot (r^\alpha)^\beta \cdot (r^\beta)^{p-1-\alpha} \pmod{p} \\ &\equiv m \cdot r^{\alpha\beta+\beta(p-1)-\alpha\beta} \pmod{p} \\ &\equiv m \cdot (r^{p-1})^\beta \pmod{p} \\ &\equiv m \cdot 1^\beta \pmod{p} \\ &\equiv m \pmod{p} \end{aligned}$$

Perhatikan bahwa eksponen $p - 1 - \alpha$ pada suku c_1 dalam dekripsi menghasilkan $(c_1^{-1})^\alpha$ tanpa memakai pangkat negatif, berdasarkan Teorema 5.1.2. □

Secara grafis:

Kriptosistem ElGamal:

Alice	di jaringan publik	Bob
pilih bilangan prima p temukan akar primitif r pilih $\alpha \mid 2 \leq \alpha \leq p-2$ hitung $a = r^\alpha \pmod p$ umumkan kunci publik	$\rightarrowtail (p, r, a)$	unduh kunci publik
terima cipherteks	$(c_1, c_2) \leftarrowtail$	diberi pesan $m \in \mathcal{M}$ (jadi $2 \leq m \leq p-1$) pilih $\beta \mid 2 \leq \beta \leq p-2$ hitung $c_1 = r^\beta \pmod p$ dan $c_2 = m \cdot a^\beta \pmod p$ kirim cipherteks
hitung plainteks $m \equiv c_2 \cdot c_1^{p-1-\alpha} \pmod p$		

ElGamal juga memiliki algoritme tanda tangan digital yang menarik:

DEFINISI 5.6.3. Misalkan Alice memiliki kunci privat ElGamal (p, r, α) dan ingin menandatangani pesan $m \in \mathcal{M}$ secara digital. Untuk setiap tanda tangan baru, mula-mula ia memilih $\gamma \in \mathbb{N}$ secara acak sehingga $1 < \gamma < p-1$ dan $\gcd(\gamma, p-1) = 1$.

Tuliskan $x = r^\gamma \pmod p$ dan $y = \gamma^{-1} \cdot (m - \alpha x) \pmod{p-1}$, dengan invers diambil modulo $p-1$. Tanda tangan digital pada m ialah pasangan (x, y).

Untuk memverifikasi tanda tangan (x, y) pada pesan m dengan kunci publik Alice (p, r, a), Bob memeriksa apakah $a^x \cdot x^y \equiv r^m \pmod p$. Jika ya, ia menerima; jika tidak, ia menolak.

Sekali lagi, kita ingin memastikan bahwa prosedur ini memberikan hasil yang semestinya.

PROPOSISI 5.6.4. *Dengan notasi di atas, Bob akan menerima setiap pesan bertanda tangan yang dihasilkan Alice menurut prosedur tersebut.*

BUKTI. Andaikan pesan bertanda tangan (m, x, y) dibuat Alice seperti di atas. Karena $y \equiv \gamma^{-1}(m - \alpha x) \pmod{p-1}$, kita mempunyai $\gamma y \equiv m - \alpha x \pmod{p-1}$. Dengan

Teorema 5.1.2, kita menghitung

$$\begin{aligned} a^x \cdot x^y &\equiv (r^\alpha)^x \cdot (r^\gamma)^y \pmod p \\ &\equiv r^{\alpha x+\gamma y} \pmod p \\ &\equiv r^{\alpha x+(m-\alpha x)} \pmod p \\ &\equiv r^m \pmod p \end{aligned}$$

Jadi, Bob akan menerima tanda tangan tersebut. □

Secara grafis:

Tanda tangan digital ElGamal:

Alice	di jaringan publik	Bob
temukan bilangan prima p dan akar primitif r pilih $\alpha \mid 2 \le \alpha \le p-2$ hitung $a = r^\alpha \pmod p$ umumkan kunci publik	$\rightarrowtail (p, r, a)$	unduh kunci publik
diberi pesan $m \in \mathcal{M}$ (jadi $2 \le m \le p-1$) pilih γ acak dengan $1 < \gamma < p-1$ dan $\gcd(\gamma, p-1) = 1$ hitung $s_1 = r^\gamma \pmod p$ dan $s_2 = \gamma^{-1} \cdot (m - \alpha s_1) \pmod{p-1}$ kirim pesan bertanda tangan	$\rightarrowtail (m, s_1, s_2)$	terima pesan bertanda tangan
		jika $a^{s_1} \cdot s_1^{s_2} \equiv r^m \pmod p$ TERIMA jika tidak, TOLAK

Latihan untuk §5.6.

LATIHAN 5.6.1. Pengajar Anda masih menyukai bilangan prima $p = 11717$ dengan akar primitif $r = 103$ dari latihan terdahulu 5.5.2 tentang DHKE. Selain itu, pengajar telah menghitung nilai $a = 1020$ untuk melengkapi kunci publik ElGamal $(p, r, a) = (11717, 103, 1020)$.

Dengan kunci publik ini, Anda ingin mengirim pesan berupa bilangan 42 kepada pengajar (bagaimanapun, itulah jawaban atas "kehidupan, alam semesta, dan segala sesuatu"). Cipherteks apa yang akan Anda kirim? Tunjukkan perhitungan Anda!

LATIHAN 5.6.2. Sekarang pengajar ingin mengirimkan nilai ujian terbaru Anda melalui surel. Untuk mendukung klaim bahwa surel itu benar-benar berasal dari pengajar, surel tersebut memuat nilai 97 beserta tambahan: "Nilai ini ditandatangani dengan tanda tangan digital ElGamal memakai kunci publik saya [kunci publik pengajar yang sama seperti dalam Latihan 5.6.1, yaitu $(p, r, a) = (11717, 103, 1020)$]; nilai tanda tangannya adalah $(6220, 10407)$."

Apakah tanda tangan itu lolos verifikasi? Dengan asumsi pengikatan identitas–kunci pengajar telah diautentikasi dan kunci privatnya tidak terkompromi, apakah Anda menerima surel tersebut sebagai benar-benar berasal dari pengajar? Tunjukkan perhitungan Anda!

LATIHAN 5.6.3. Buat kunci publik ElGamal dan kirimkan kepada pengajar melalui surel. Tunggu pesan balasan yang dienkripsi dengan ElGamal, lalu kirim kembali plainteksnya kepada pengajar.

Selain itu, gunakan kunci publik Anda untuk menandatangani bilangan 17 sebagai pesan. Kirimkan bilangan bertanda tangan itu kepada pengajar dan tunggu kabar apakah tanda tangannya diterima atau ditolak.

Daftar Pustaka

[AB09] Sanjeev Arora and Boaz Barak, *Computational Complexity: A Modern Approach*, Cambridge University Press, 2009.

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, *Primes is in p*, Annals of mathematics (2004), 781–793.

[Bou04] Nicolas Bourbaki, *Theory of sets*, Springer, 2004.

[DH76] Whitfield Diffie and Martin E Hellman, *New directions in cryptography*, Information Theory, IEEE Transactions on **22** (1976), no. 6, 644–654.

[FS03] Niels Ferguson and Bruce Schneier, *Practical cryptography*, vol. 23, Wiley New York, 2003.

[Gau86] Carl Friedrich Gauß, *Disquisitiones Arithmeticae, 1801. English translation by Arthur A. Clarke*, 1986.

[Har05] Godfrey Harold Hardy, *A Mathematician's Apology*, 2005, First electronic edition, available at `http://www.math.ualberta.ca/mss`.

[HC] Dan Harkins and Dave Carrel, *RFC 2409: The Internet Key Exchange (IKE), November 1998*, Status: Proposed Standard.

[HW79] Godfrey Harold Hardy and Edward Maitland Wright, *An introduction to the theory of numbers*, Oxford University Press, 1979.

[LK08] M Lepinski and S Kent, *RFC 5114-Additional Diffie-Hellman Groups for Use with IETF Standards*, 2008.

[Lub96] Michael George Luby, *Pseudorandomness and Cryptographic Applications*, Princeton University Press, 1996.

[MVOV96] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone, *Handbook of applied cryptography*, CRC press, 1996.

[NC10] Michael A Nielsen and Isaac L Chuang, *Quantum computation and quantum information*, Cambridge university press, 2010.

[PS04] Jonathan A Poritz and Morton Swimmer, *Hash woes*, Virus Bulletin (2004), 14–16.

[RSA78] Ronald L Rivest, Adi Shamir, and Len Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126.

[Sha48] C. E. Shannon, *A mathematical theory of communication*, Bell Systems Technical Journal **27** (1948), 379–423, 623–656.

[Sha49] ———, *Communication theory of secrecy systems*, Bell System Technical Journal **28** (1949), no. 4, 656–715.

[Sho94] Peter W Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, IEEE, 1994, pp. 124–134.

[Sho09] Victor Shoup, *A computational introduction to number theory and algebra*, Cambridge University Press, 2009, on-line at `http://shoup.net/ntb/`.

[Sta02] Richard Stallman, *Free Software, Free Society: Selected Essays of Richard M. Stallman*, Lulu.com, 2002.

[WY05] Xiaoyun Wang and Hongbo Yu, *How to break md5 and other hash functions*, Advances in Cryptology–EUROCRYPT 2005, Springer, 2005, pp. 19–35.

Indeks